UNIVERSITÀ DEGLI STUDI
DELL'INSUBRIA

REGOLAMENTO
PER L'ACCESSO E L'UTILIZZO
DELLE INFRASTRUTTURE CENTRALI DI
INFORMATION E *COMMUNICATION TECHNOLOGY* (ICT)
DELL'ATENEO

Emanato con Decreto Rettorale 22 marzo 2019, n. 203
Ultime modifiche emanate con Decreto Rettorale 5 settembre 2022, n. 788
Entrate in vigore il 6 settembre 2022

AREA SISTEMI INFORMATIVI
Via Ravasi, 2 – 21100 Varese (VA) – Italia
Web: www.uninsubria.it
P.I. 02481820120 - C.F. 95039180120
Chiaramente Insubria!

INDICE

Premesse

Art. 1 - Oggetto e finalità

L'Università degli Studi dell'Insubria promuove l'utilizzo degli strumenti di *Information e Communication Technology* per il perseguimento dei propri fini istituzionali legati allo sviluppo, promozione e diffusione della conoscenza. Il presente Regolamento disciplina le modalità di utilizzo, accesso e conduzione dei servizi ICT.
Il presente Regolamento è emanato in conformità con quanto previsto dalla normativa in materia di servizi ICT[1].

Art. 2 - Definizioni

1. Consortium GARR: organizzazione che gestisce la rete italiana delle università e della ricerca, garantendone l'ampliamento e lo sviluppo anche attraverso attività di ricerca tecnologica nel campo del *networking*, curandone l'interconnessione con tutte le reti dell'istruzione e della ricerca internazionali e con la rete internet commerciale.
2. AUP del Consortium GARR: *Acceptable Use Policy* del Consortium GARR (http://www.garr.it/a/utenti/regole-di-accesso/acceptable-use-policy-aup).
3. Struttura: Amministrazione Centrale, Dipartimento, Centri Speciali, Scuola di Medicina.
4. *Host*: *computer*, terminale, stampante, periferica, telefono, fax o dispositivo.
5. Rete dati di Ateneo (RDA): l'insieme delle infrastrutture fisiche e logiche e dei servizi che consente la comunicazione e la trasmissione di dati e fonia sia all'interno che all'esterno dell'Ateneo.
6. Presa utente: nodo terminale della RDA, al quale può essere collegato un *host*.
7. Sistemi telefonici: apparecchi telefonici fissi e mobili, centralini e relativi *software*, collegamenti telefonici interni ed esterni, dispositivi *wireless* per la fonia.
8. Amministratore della RDA: l'Area Sistemi Informativi è incaricata della gestione amministrativa e tecnica della RDA, dei domini "uninsubria.it" e "uninsubria.eu" e dello spazio di indirizzamento IP assegnato all'Ateneo dal Consortium GARR.
9. Responsabile di struttura: Direttore Generale, Direttore di Dipartimento, Responsabile dell'Area Sistemi Informativi, Direttore di centro speciale, Presidente di Scuola di specializzazione.
10. Utente interno: titolare di identità digitale di cui all'art.5 commi 1-5.
11. SicOnLine: portale *Web* SIC on Line (http://w3.ateneo.uninsubria.it/)
12. VPN: *Virtual Private Network*
13. Responsabile per la transizione digitale: nominato dall'Ateneo ai sensi dell'art. 17 del D. Lgs 5 marzo 2005, n. 82 e ss.mm.ii (Codice Amministrazione Digitale) ha la funzione di garantire la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Ai sensi dell'art. 17, comma 1, lett. c) del D. Lgs 82/2005

[1] Cfr Allegato C

gli sono attribuiti compiti di *indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1*.

14. Misure minime di sicurezza informatica per le pubbliche amministrazioni. Università degli Studi dell'Insubria. Documento redatto ai sensi della Circolare 18 aprile 2017, n. 2 dell'Agenzia per l'Italia Digitale – AgID.
15. ABSC: AgID *Basic Security Control(S).*
16. GDPR: Regolamento Europeo per la Protezione dei Dati (Regolamento UE 679/16)
17. Incidente Informatico: incidente che impatta o minaccia di impattare sul regolare funzionamento di uno o più sistemi o dispositivi informatici.
18. Incidente Informatico di Sicurezza: incidente informatico verificatosi a seguito di una violazione della politica aziendale oppure della normativa vigente in materia di sicurezza informatica.
19. *Data Breach*: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
20. DPO: Responsabile della Protezione dei dati Personali ai sensi dell'art. 37 del Regolamento dell'Unione Europea (UE) 2016/6.

Titolo I - IDENTITÀ DIGITALI DI ATENEO

Art. 3 - Le identità digitali di Ateneo

1. L'identità digitale è costituita da informazioni o qualità di un utente, denominate attributi, utilizzate per rappresentarne l'identità, lo stato, la forma giuridica o altre caratteristiche peculiari ed è verificata attraverso un sistema di identificazione e autenticazione informatica.
2. Le identità digitali di Ateneo sono costituite da nome utente, *password*, dati personali, informazioni sulla carriera e altri dati a uso esclusivo dei sistemi e delle procedure informatiche.
3. L'identità digitale è strumentale all'accesso a uno o più servizi telematici.
4. L'Ateneo favorisce la partecipazione alle Federazioni di Autenticazione previste dall'ordinamento nazionale (SPID) o in uso sulle reti dell'università e della ricerca a livello nazionale, europeo e mondiale, quale ad esempio Eduroam, che operano in una logica di identità federate.

Art. 4 - Attributi dell'Identità Digitale di Ateneo

1. Gli attributi sono divisi in cinque categorie:
    a. caratteristiche personali;
    b. posta elettronica;
    c. riferimenti alla carriera studente;
    d. riferimenti alla carriera del personale;
    e. altro.

Art. 5 - Titolari delle Identità Digitali di Ateneo

I titolari delle identità digitali di Ateneo sono ricompresi nelle seguenti categorie:

1. Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica;
2. Professori Emeriti, Professori Onorari;
3. Professori Senior e Ricercatori Senior;
4. Collaboratori e consulenti titolari di un contratto con l'Ateneo;
5. Altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo;
6. Registrati a corsi di studio magistrale non ciclo unico, immatricolati e iscritti a corsi di studio, iscritti a master e corsi di perfezionamento;
7. Registrati al sistema di gestione delle carriere degli studenti;
8. Studenti iscritti a corsi di dottorato o di specializzazione;
9. Studenti immatricolati in Università straniere in scambio presso l'Ateneo;

10. Referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo;

Art. 6 - Ciclo di vita dell'Identità digitale di Ateneo

1. La creazione di una identità digitale, comporta un trattamento dei dati la cui liceità si basa sull'art. 6, comma 1, lett. b), c), e) del Regolamento UE 679/2016[2], e avviene:
   - Per personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, collaboratori e consulenti titolari di un contratto con l'Ateneo ed altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo l'identità è creata alla data di decorrenza del contratto, registrata dall'ufficio competente nei sistemi informativi per la gestione delle risorse umane.
   - Per Professori Emeriti, Professori Onorari, Professori Senior e Ricercatori Senior, l'identità è creata a seguito del conferimento del ruolo a cura degli organi preposti.
   - Per gli studenti Registrati al sistema di gestione delle carriere degli studenti e studenti immatricolati in Università straniere in scambio presso l'Ateneo, l'identità digitale è creata al momento della registrazione nel sistema di gestione degli studenti.
   - Per referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo, l'identità digitale è creata dopo l'approvazione della richiesta di attivazione formulata dal Responsabile Unico del Procedimento (RUP) o dal responsabile del servizio ed inviata al Responsabile dell'Area Sistemi Informativi, corredata delle relative motivazioni, che ne valuterà l'ammissibilità.
2. L'attivazione dell'identità digitale per personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Professori Emeriti, Professori Onorari, Professori Senior, Ricercatori Senior, collaboratori e consulenti titolari di un contratto con l'Ateneo, titolari di altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo, è effettuata dal titolare della identità digitale dopo aver ricevuto notifica della creazione della propria identità digitale di Ateneo. Per gli studenti e gli assimilati (di cui all'art. 5, comma 6, 7, 8, 9) l'attivazione dell'identità digitale è contestuale alla sua creazione. Per i referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con

[2] Regolamento (UE) 679/2016 art, 6, comma 1, lett. b) *il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso,* lett. c) *il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento,* lett. e) *il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.*

l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo, l'attivazione dell'identità digitale è contestuale alla sua creazione.

3. La disattivazione dell'identità digitale, avviene nel momento in cui a essa non sono più associate autorizzazioni per accedere a servizi dell'Ateneo. Nello stato 'disattivato' l'identità digitale verrà svuotata di tutti gli attributi non più necessari all'erogazione dei servizi.

- Per personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, collaboratori e consulenti titolari di un contratto con l'Ateneo, titolari di altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo, la disattivazione dell'identità digitale è effettuata dopo 12 mesi dalla scadenza del contratto;
- Per Professori Emeriti, Professori Onorari, Professori Senior e Ricercatori Senior l'identità digitale rimarrà attiva sino al perdurare dello status Professori Senior e Ricercatori Senior, al termine del quale la disattivazione verrà effettuata dopo 12 mesi;
- Per gli studenti e gli assimilati (di cui all'art. 5, comma 6, 7, 8, 9) l'identità digitale rimarrà attiva a tempo indeterminato;
- Per i referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo, l'identità digitale è disattivata al cessare delle motivazioni che ne hanno comportato l'attivazione o alla scadenza del contratto ad essa associato.

4. La cancellazione dell'identità digitale sarà effettuata esclusivamente su richiesta del titolare. All'atto della comunicazione di scadenza dell'identità digitale al soggetto titolare sarà data comunicazione circa i modi per ottenere la cancellazione dei dati dal *data base* dell'Ateneo. In assenza di precisa richiesta di cancellazione i dati saranno conservati dall'Ateneo al solo scopo di evitare la riassegnazione di un identificativo e/o di un indirizzo di posta elettronica a un soggetto omonimo.

Art. 7 - Ciclo di vita delle Autorizzazioni di accesso ai servizi

Attivazione dei Servizi

1. All'atto di attivazione dell'identità digitale, sono assegnati alcuni servizi di base come indicato di seguito:

- A Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Professori Emeriti, Professori Onorari, Professori Senior, Ricercatori Senior, collaboratori e consulenti titolari di un contratto con l'Ateneo, titolari di altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo, con l'attivazione dell'identità digitali sono contestualmente attivi:

accesso alla rete *wifi*, accesso al portale SicOnLine, posta elettronica, accesso alle postazioni dei laboratori informatici e delle biblioteche.

- Per gli studenti registrati al sistema di gestione delle carriere degli studenti Utenze, è automaticamente attivato l'accesso al portale *web* di gestione della carriera di studio WebESSE3;
- Per gli studenti registrati a corsi di studio magistrale non ciclo unico, immatricolati e iscritti a corsi di studio, iscritti a master e corsi di perfezionamento, vengono attivati: l'accesso al portale *web* di gestione della carriera di studio WebESSE3, Elearning, posta elettronica, accesso alla rete *wifi*, accesso alle postazioni dei laboratori informatici e delle biblioteche;
- Per gli studenti immatricolati in Università straniere in scambio presso l'Ateneo, sotto attivati. all'atto della registrazione nel sistema di gestione della carriera di studi (Esse3): l'accesso al portale *web* di gestione della carriera di studio WebESSE3, accesso alla rete *wifi*, accesso alle postazioni dei laboratori informatici e delle biblioteche;
- Per i referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi dell'Ateneo, con l'attivazione dell'identità digitali sono contestualmente attivi: accesso alla rete *wifi*.

2. Tutti gli ulteriori servizi, non contemplati sopra, sono attivati solo previa puntuale richiesta dell'utente interessato con modalità specifiche per i singoli servizi.

Disattivazione dei Servizi

3. La revoca dei servizi assegnati avviene in modalità automatica secondo le seguenti regole:

- Per personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Collaboratori e consulenti titolari di un contratto con l'Ateneo, Altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo, referenti di enti, associazioni o società:
    a. accesso al portale SicOnLine, accesso alle postazioni dell'Amministrazione Centrale, accesso agli applicativi Gestionali e Documentali centrali: alla cessazione del contratto;
    b. posta elettronica, accesso alla rete *wifi,* accesso al portale E-Learning, accesso alle postazioni dei laboratori informatici e delle biblioteche: 12 mesi al termine del contratto.
- Professori Senior e Ricercatori Senior:
    a. accesso al portale SOL: alla decadenza dallo status di Professori Senior e Ricercatori Senior;
    b. posta elettronica, accesso alla rete *wifi,* accesso al portale E-Learning, accesso alle postazioni dei laboratori informatici e delle biblioteche: 12 mesi dalla decadenza dallo status di Professori Senior e Ricercatori.

- Studenti immatricolati a corsi di studio, iscritti a master e corsi di perfezionamento, Studenti iscritti a corsi di dottorato o di specializzazione, Studenti immatricolati in Università straniere in scambio presso l'Ateneo:
    a. posta elettronica, accesso alla rete *wifi,* accesso al portale E-Learning, accesso alle postazioni dei laboratori informatici e delle biblioteche: 12 mesi dopo cessazione per conseguimento titolo, rinuncia, trasferimento, decadenza o termine carriera;
    b. accesso in modalità remota alle banche dati e riviste elettroniche Area Servizi Bibliotecari e documentali: alla cessazione per conseguimento titolo, rinuncia, trasferimento, decadenza o termine carriera;
    c. accesso WebESSE3: attivo a tempo indeterminato.

- Utenze assegnate a persone registrate a corsi di studio magistrali:
    a. posta elettronica: entro il 30 aprile dell'anno successivo alla registrazione, se questa non è stata perfezionata con l'immatricolazione.

4. I servizi a richiesta vengono revocati in modalità manuale nel momento in cui decade il diritto di fruirne.
5. Tutti i servizi possono essere revocati con decorrenza immediata nel caso in cui venga meno il rapporto di fiducia con l'Ateneo (ad esempio in caso di licenziamento per giusta causa, illecito disciplinare, utilizzo illecito dei servizi), la disattivazione dei servizi associati all'identità digitale è distinguibile fra servizi assegnati e servizi a richiesta.

Art. 8 - Politica di Sicurezza per le Identità digitali di Ateneo

1. Le identità digitali di Ateneo sono memorizzate sui sistemi informatici dall'Area Sistemi Informativi che provvede ad implementare le misure idonee per garantirne l'integrità, la confidenzialità e la disponibilità delle identità digitali nel tempo. Le *password* associate alle identità digitali, devono essere memorizzate esclusivamente in modalità cifrata e non reversibile, con livelli di sicurezza adeguati agli standard di mercato.
2. I sistemi informatici, informativi e di comunicazione, che utilizzano le identità digitali di Ateneo per i processi di autenticazione e, eventualmente, di autorizzazione, devono essere configurati per garantirne la confidenzialità e l'integrità dell'identità digitale e quella dei suoi attributi eventualmente veicolati. Per nessun motivo devono essere memorizzate su sistemi di terzi le credenziali di autenticazione delle identità digitali di Ateneo (*password*). Per le indicazioni di natura tecnologica e i protocolli di comunicazioni supportati, si rimanda all'Allegato A.
3. Il titolare dell'identità digitale ha l'onere e la responsabilità di adottare le misure e i comportamenti idonei per garantirne la confidenzialità. In particolare i titolari non devono comunicare o rendere accessibile a terzi la *password* associata all'identità, devono utilizzare *password* sicure in base alle buone prassi vigenti (quali, ad esempio, lunghezza non inferiore ad 8 caratteri, non contenente riferimenti anagrafici del

titolare dell'identità, contenente almeno un carattere speciale, etc.) devono provvedere al cambio periodico della *password*. Nel caso in cui il titolare dell'identità utilizzi la stessa per accedere a banche dati che trattano dati sensibili o giudiziari dovrà provvedere a cambiare la *password* almeno ogni 90 giorni solari, in forza del principio di *accountability* previsto dall'art. 32 del GDPR.

4. L'Area Sistemi Informativi nel caso in cui l'identità digitale sia utilizzata per accedere a banche dati di Ateneo gestite dall'Area stessa e che trattino dati sensibili o giudiziari ai sensi dell'art. 32 del GDPR, implementa politiche di sicurezza centralizzate che comportano l'obbligo del cambio *password* entro 90 giorni e l'utilizzo di *password* con adeguati livelli di complessità, in forza dell'art. 32 del GDPR.

Art. 9 - Interoperabilità con le Identità digitali di Ateneo

Le Identità digitali di Ateneo possono essere utilizzate per i processi di autenticazione ed eventualmente di autorizzazione per i servizi informatici e telematici erogati dall'Ateneo tramite infrastrutture e servizi informatici gestiti direttamente o affidati a terzi. Le modalità di interoperabilità sono definite nell'Allegato A.

Titolo II - RETE DATI DI ATENEO

L'Università degli Studi dell'Insubria considera la RDA un elemento strategico e fondamentale per il perseguimento dei propri fini istituzionali e ne promuove lo sviluppo, il buon funzionamento e la sicurezza.

Art. 10 - Amministratore della Rete di Ateneo

1. L'Amministratore della RDA assicura in modo esclusivo e tempestivo la gestione, il monitoraggio, l'aggiornamento e ampliamento della RDA sia sotto l'aspetto fisico che logico, curandone i relativi progetti, fino alla "presa utente" compresa.
5. L'Amministratore della RDA, nell'espletamento dei propri compiti di gestione e monitoraggio della RDA, ha la facoltà di raccogliere dati relativi alle attività di rete degli *host* ad essa collegati secondo le modalità specificate nel presente Regolamento.
6. L'Amministratore della Rete di Ateneo ha la facoltà di revocare temporaneamente l'autorizzazione di accesso alla RDA o limitarne la fruizione da parte di uno o più *host* secondo quanto previsto dall'art. 27 comma 9.

Art. 11 - Referenti informatici di struttura

1. Ogni struttura che abbia uno o più *host* connessi alla RDA deve nominare uno o più Referenti informatici e comunicarne i nominativi all'Amministratore della RDA.
2. Un Referente informatico può essere condiviso fra più strutture.
3. Una struttura può nominare un soggetto esterno qualificato quale Referente informatico di struttura.
4. Il Responsabile di ciascuna struttura deve comunicare tempestivamente all'Amministratore della RDA eventuali cambiamenti del nominativo del Referente informatico di struttura.
5. I Referenti informatici di struttura rappresentano il punto di contatto amministrativo e tecnico degli utenti di ciascuna struttura con l'Amministratore della RDA e hanno l'obbligo di riferirsi all'Amministratore della RDA in caso di violazione o sospetto di violazione della sicurezza informatica e/o del presente regolamento.
6. In caso di problemi di sicurezza informatica causati dagli *host* della struttura di afferenza connessi alla RDA i Referenti informatici di struttura collaborano con l'Amministratore della RDA eseguendo le eventuali istruzioni e procedure ricevute dall'Amministratore della RDA.
7. I Referenti informatici non intervengono di propria iniziativa sulle apparecchiature di rete e sul cablaggio strutturato della RDA.

Art. 12 - Utenti della Rete Dati di Ateneo

1. Hanno diritto di collegare dispositivi sulla rete via cavo dell'Ateneo (RDA):
    a. Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Professori Emeriti, Professori Onorari, Professori Senior, Ricercatori Senior,

collaboratori e consulenti titolari di un contratto con l'Ateneo, titolari di altre forme di collaborazione in cui l'attività lavorativa sia prevalentemente svolta presso l'Ateneo, studenti iscritti a corsi di dottorato o di specializzazione, referenti di enti, associazioni o società esterne che collaborano a qualunque titolo con l'Ateneo e che abbiano necessità di accedere ad alcuni servizi offerti dai sistemi informativi, per i quali è attiva una identità digitale di Ateneo;

b. il personale di Enti pubblici o privati coinvolti in attività oggetto di convenzioni con l'Università limitatamente alla durata e ai fini della relativa collaborazione;
c. gli utenti "ospiti" di cui al successivo art. 13;
d. partecipanti ad eventi istituzionali organizzati presso l'Ateneo di cui al successivo art. 14;
e. gli utenti delle federazioni e confederazioni cui l'Ateneo aderisce con le modalità e limitazioni previste dai regolamenti d'uso.

2. Tutti gli utenti della RDA sono responsabili delle attività svolte attraverso la RDA e sono tenuti all'osservanza della normativa vigente nazionale e comunitaria, del presente regolamento e delle regole stabilite dall'AUP del Consortium GARR.
3. Tutti gli utenti della RDA sono tenuti a segnalare immediatamente all'Amministratore della RDA o al Referente informatico di struttura ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

Art. 13 - Utenti ospiti

1. Sono considerati ospiti le persone accolte e/o invitate per un tempo determinato da personale dell'Ateneo presso strutture dell'Ateneo per attività istituzionali o comunque strettamente correlate e funzionali all'Ateneo.
2. Agli ospiti sono forniti i seguenti servizi: accesso alla rete *wireless* dedicata agli ospiti, accesso alle postazioni di lavoro dei laboratori informatici e delle biblioteche, possibilità di collegare alla rete *wired* dell'Ateneo un proprio dispositivo.
3. L'accesso ai servizi da parte degli ospiti avviene previa autenticazione con credenziali rilasciate dall'Ateneo.
4. La richiesta delle credenziali di accesso per gli ospiti deve essere inoltrata all'Amministratore della RDA da un utente interno attraverso gli strumenti di supporto messi a disposizione dall'Area Sistemi Informativi.
5. Gli ospiti sono sempre riferibili a una persona legata da un rapporto contrattuale con l'Ateneo, che si assume la responsabilità di identificarli, ospitarli, di verificare che esistano i presupposti per la permanenza degli stessi presso i locali dell'Ateneo e che l'utilizzo delle risorse IT messe a loro disposizione avvenga in conformità ai vigenti regolamenti dell'Ateneo. L'utente interno è inoltre responsabile della veridicità delle informazioni dichiarate nella richiesta di cui al comma precedente.

Art. 14 - Partecipanti a eventi

1. Ogni evento dovrà avere un responsabile individuato fra le persone legate da un rapporto contrattuale con l'Ateneo; il responsabile dell'evento si potrà eventualmente avvalere di una segreteria alla quale delegare alcuni aspetti organizzativi.
2. Il responsabile dell'evento può richiedere l'accesso ai servizi *UninsubriaWireless* per i partecipanti.
3. I partecipanti a eventi, sono le persone regolarmente iscritte o comunque titolate a partecipare a eventi organizzati dall'Ateneo.
4. Ai partecipanti a eventi dell'Ateneo è concesso l'accesso alla rete *wifi* dedicata e previa autenticazione.

Art. 15 - Connessione di *host* alla Rete Dati di Ateneo

1. Per collegare un *host* alla RDA è necessario inoltrare una specifica richiesta all'Amministratore della RDA, in conformità a quanto richiesto dalle *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*[3], che rilascerà un indirizzo IP anche tramite servizi DHCP automatizzati[4].
2. Nella richiesta di cui al comma 1 del presente articolo, qualora l'*host* sia destinato all'erogazione di servizi, questi dovranno essere debitamente dichiarati come previsto dalle *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*.
3. La richiesta di collegare un *host* alla RDA, di cui al comma 1 del presente articolo, può essere inoltrata esclusivamente dagli utenti dotati di identità digitale di Ateneo appartenenti alle categorie di cui all'art. 5 commi 1, 2, 3, 4 e 7 attraverso il servizio disponibile sul portale SOL. Nel caso la richiesta venga effettuata dal Responsabile di Struttura, direttamente o mediante un proprio delegato, l'*host* sarà assegnato alla Struttura e la responsabilità sarà attribuita al Responsabile della Struttura stessa negli altri casi la responsabilità dell'*host* è attribuita al titolare dell'identità digitale di Ateneo che ha effettuato la richiesta.
4. Attraverso i servizi del portale SOL gli utenti dotati di identità digitale di Ateneo appartenenti alle categorie Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Professori Emeriti, Professori Onorari, Professori Senior e Ricercatori Senior, Collaboratori e consulenti titolari di un contratto con l'Ateneo possono inoltrare la richiesta di cui al comma 1 del presente articolo per conto degli "utenti ospiti", così come definiti all'art. 13, comma 1. In questo caso la responsabilità dell'*host* è attribuita al titolare dell'identità digitale di Ateneo che ha effettuato la richiesta.

[3] Agenzia per l'Italia Digitale – AgID "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)", Circolare 17 aprile 2017, n. 2/2017.

[4] DHCP: servizio di assegnazione automatica degli indirizzi di rete (IP) grazie al quale un client di rete richiede a un *server* centrale l'assegnazione di un indirizzo il quale procede al rilascio dell'indirizzo IP in base alle logiche implementate per la rete specifica da cui proviene la richiesta ed alla disponibilità contingente degli indirizzi.

5. Attraverso i servizi del portale SOL gli utenti dotati di identità digitale di Ateneo appartenenti alle categorie Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Professori Emeriti, Professori Onorari, Professori Senior e Ricercatori Senior, Collaboratori e consulenti titolari di un contratto con l'Ateneo possono inoltrare la richiesta di cui al comma 1 del presente articolo per collegare *host* di proprietà di soggetti esterni che eroghino servizi in rete nell'ambito di una fornitura all'Ateneo. In questo caso la responsabilità dell'*host* è attribuita al titolare dell'identità digitale di Ateneo che ha effettuato la richiesta.
6. All'utente, titolare dell'identità digitale di Ateneo, che ha formulato la richiesta di connessione dell'*host di cui al comma 1 del presente articolo per le categorie utenti ospiti e/o* soggetti esterni che eroghino servizi in rete nell'ambito di una fornitura all'Ateneo, è attribuita la responsabilità della veridicità delle informazioni dichiarate in tale richiesta.
7. È espressamente vietata l'auto-assegnazione dell'indirizzo IP.
8. Al titolare di identità digitale di Ateneo, appartenente alle categorie Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, Professori Emeriti, Professori Onorari, Professori Senior e Ricercatori Senior, Collaboratori e consulenti titolari di un contratto con l'Ateneo e Registrati al sistema di gestione delle carriere degli studenti che abbia effettuato richiesta di collegamento di un host all'RDA di cui al comma 1 del presente articolo, è attribuita la responsabilità relativa a tutti gli adempimenti necessari al rispetto del presente Regolamento, della legislazione europea e nazionale vigente, e in particolare agli adempimenti relativi al rispetto della Circolare dell'Agenzia per l'Italia Digitale - AgID 17 aprile 2017, n. 2, *Misure minime di sicurezza ICT per le pubbliche amministrazioni,* specificatamente per quanto concerne le ABSC 5.7.1, 5.7.3, 8.1.1, 8.1.2, 8.7.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1 e 13.1.1.[5] Il perfezionamento della richiesta è subordinato all'esplicita accettazione delle condizioni di utilizzo della RDA e all'assunzione di responsabilità circa gli adempimenti di cui al presente comma.
9. Al Responsabile di Struttura, che abbia effettuato la richiesta di collegamento di un host all'RDA di cui al comma 1 del presente articolo, è attribuita la responsabilità relativa a tutti gli adempimenti necessari al rispetto del presente Regolamento, della legislazione europea e nazionale vigente, e in particolare agli adempimenti relativi al rispetto della Circolare dell'Agenzia per l'Italia Digitale - AgID 17 aprile 2017, n. 2, *Misure minime di sicurezza ICT per le pubbliche amministrazioni.* Il Responsabile della struttura, come previsto dalla normativa, dovrà trasmettere al Responsabile per la transizione digitale, nominato dall'Ateneo ai sensi dell'art. 17 del D. Lgs 5 marzo 2005, n. 82 e ss.mm.ii (Codice Amministrazione Digitale), il documento[6], compilato secondo lo schema predisposto da AgID, con cui deve essere attestato il grado di implementazione delle *Misure minime di sicurezza ICT* sugli *host* della struttura di cui è

[5] In Allegato D il dettaglio delle Misure Minime di sicurezza ICT per le pubbliche amministrazioni relative alle ABSC richieste al comma 8

[6] In Allegato E lo schema predisposto da AgiD per la definizione del grado di implementazione delle misure minime di sicurezza. Il documento dovrà essere sottoscritto con firma digitale.

responsabile. In mancanza di tale documento o qualora il livello di implementazione delle *Misure minime di sicurezza ICT* non sia conforme a quanto stabilito dalla normativa e coerente con il piano di adeguamento dell'Ateneo, il Responsabile per la transizione digitale può disporre, in attesa che siano effettuati i necessari interventi di adeguamento, la temporanea inibizione dell'accesso per gli *host* afferenti alla Struttura. Il Responsabile della Struttura dovrà aggiornare tale documento ogni qualvolta intervengano modifiche degli *host* e delle relative configurazioni o qualora ciò venga richiesto dal Responsabile per la transizione digitale.

10. Al fine di garantire adeguati livelli di sicurezza e la verifica di validità delle utenze abilitate l'autorizzazione di accesso degli *host* alla RDA può essere soggetta a revisione periodica. L'Amministratore della RDA, con congruo preavviso può richiedere agli intestatari degli *host* di riconfermarne la titolarità e il permanere dei presupposti di diritto di accesso alla RDA. In caso di mancata risposta l'Amministratore della RDA può revocare tale autorizzazione.

Art. 16 - Connessione di dispositivi IoT

Tutti i dispositivi informatici (IoT) incorporati in oggetti di uso comune con lo scopo di inviare e ricevere dati attraverso Internet, quali a titolo di esempio non esaustivo: sensori di rilevamento, lettori di banda magnetica o RFID, telecamere IP, centraline e termostati, ecc:

1. possono essere connessi alla RDA secondo le modalità definite all'art. 15.
2. nella richiesta è obbligatorio dichiarare i servizi erogati dal dispositivo così come prescritto all'art. 15, comma 2.
3. i dispositivi appartenenti alla categoria IoT verranno collegati su reti di accesso dedicate e separate dalle reti su cui sono collegati *server*, *desktop* e *notebook*.
4. l'accesso alla rete IoT può essere implementato da *host* connessi alla rete di accesso della RDA esclusivamente attraverso *gateway* e protocolli sicuri.
5. le reti IoT di norma non consentono l'accesso a Internet e non sono accessibili da Internet. La richiesta di eventuale deroga a tale norma deve essere debitamente motivata, deve essere garantito un adeguato livello di sicurezza ed è subordinata all'autorizzazione dell'Amministratore della RDA.

Art. 17 - Connessione di laboratori informatici e postazioni pubbliche alla Rete dati di Ateneo

1. La connessione alla RDA di postazioni dei laboratori informatici, postazioni pubbliche o altre tipologie di aree attrezzate deve essere esplicitamente autorizzata dall'Amministratore della RDA poiché soggetta alle ulteriori specifiche regolamentazioni di cui al comma 3 del presente articolo.
2. La richiesta di autorizzazione, sottoscritta dal Responsabile di struttura, è scaricabile dal portale SOL e deve riportare le seguenti informazioni obbligatorie:
    a. nominativo di una persona responsabile della gestione tecnica;

   b. descrizione del laboratorio o delle postazioni pubbliche e indicazione dell'utilizzo prevalente;
   c. elenco delle prese utente a cui saranno collegati gli *host*.
3. I laboratori informatici e le postazioni pubbliche sono soggette alle seguenti specifiche regolamentazioni:
   a. alle postazioni, salvo casi debitamente documentati, sono assegnati indirizzi IP privati;
   b. l'accesso alla RDA deve avvenire tramite un sistema, frapposto tra le postazioni e la RDA, che limiti l'accesso alle sole risorse autorizzate e tenga traccia di eventuali violazioni;
   c. deve essere possibile limitare l'utilizzo di banda da parte delle postazioni al fine di preservare il buon funzionamento della RDA nel suo complesso;
   d. gli utenti non devono accedere al sistema con i privilegi di amministratore, salvo motivate eccezioni, e non devono installare applicativi di qualsiasi genere;
   e. gli applicativi utilizzabili dall'utente devono essere soltanto quelli consentiti e concordati con il Referente informatico di struttura;
   f. i gestori di laboratori o postazioni pubbliche connesse alla RDA devono provvedere alla raccolta e conservazione dei log di accesso in conformità alla normativa vigente e a quanto definito nel Titolo VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG;
   g. nei log di cui al punto precedente sono contenuti i riferimenti temporali e gli identificativi delle postazioni e degli utenti che hanno effettuato l'accesso.

Art. 18 - Connessione di *host* alla rete UninsubriaWireless

1. L'Area Sistemi Informativi gestisce e mette a disposizione in tutti gli stabili dell'Ateneo il servizio di accesso *wireless* denominato "*UninsubriaWireless*".
2. Le reti *wifi* sono tipicamente reti di accesso a cui sono connessi dispositivi personali (BYOD[7]). Tali reti sono da considerarsi potenzialmente insicure e sono di conseguenza soggette a restrizioni rispetto all'accesso ai sistemi informatici o applicativi dell'Ateneo i quali necessitino di più stringenti livelli di sicurezza in considerazione della tipologia dei dati trattati e/o dell'importanza strategica ad essi attribuita.
3. Nelle aree coperte dal servizio *UninsubriaWireless*, è possibile accedere alla Rete dati di Ateneo in modalità *wireless* esclusivamente previa autenticazione utilizzando:
   - le credenziali associate all'identità digitale di Ateneo di cui agli artt. 3 e 5;
   - le credenziali per utente ospite di cui all'art. 13;
   - le credenziali per partecipanti ad eventi di cui all'art. 14;
   - le credenziali istituzionali del proprio ente di appartenenza per gli utenti della Federazione internazionale Eduroam

[7] BYOD *Bring Your Own Device*

4. L'Amministratore della RDA raccoglie e conserva i log di accesso della rete *UninsubriaWireless*, in conformità alla normativa vigente e a quanto definito nel Titolo VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.
5. Nei log di cui al comma precedente sono contenuti i riferimenti temporali e gli identificativi delle postazioni e degli utenti che hanno effettuato l'accesso.

Art. 19 - Realizzazione di reti *wireless* per l'accesso alla Rete dati di Ateneo

1. L'implementazione di una rete *wireless* comporta a tutti gli effetti un'estensione della RDA. Una struttura può implementare una rete *wireless* solo dopo aver ottenuto l'autorizzazione dall'Amministratore della RDA.
2. L'autorizzazione alla realizzazione di una rete *wireless* è rilasciata a seguito della valutazione della richiesta di cui al comma precedente da parte dell'Amministratore della RDA. La realizzazione di reti *wireless* deve essere giustificata da una effettiva esigenza che richieda questo tipo di soluzione, in ragione degli inconvenienti che tale scelta comporta (basse velocità, intercettabilità, estensione del campo d'azione al di fuori dei confini universitari, sicurezza).
3. Per quanto riguarda la sicurezza, l'implementazione della soluzione *wireless* deve garantire l'accesso soltanto agli utenti abilitati (autenticazione) e deve prevedere la crittazione del traffico (riservatezza), per portare il livello di sicurezza di questo tipo di reti allo stesso livello garantito da quelle cablate.
4. I gestori di reti *wireless* connesse alla RDA devono provvedere alla raccolta e conservazione dei log di accesso in conformità alla normativa vigente e a quanto definito nel Titolo VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.
5. I log di cui al comma precedente devono contenere i riferimenti temporali e gli identificativi delle postazioni e degli utenti che hanno effettuato l'accesso.

Art. 20 - Accesso remoto alla Rete dati di Ateneo in modalità VPN *Client to Site*

1. L'Amministratore della RDA gestisce il servizio di accesso remoto alla RDA mediante VPN per il personale in regime di telelavoro.
2. L'accesso da remoto alla RDA deve avvenire esclusivamente utilizzando protocolli sicuri e che garantiscano l'integrità e la confidenzialità dei dati veicolati su Internet.
3. Gli amministratori di servizi di accesso remoto in modalità VPN o assimilata (quali ad esempio *SSH tunnel*) devono raccogliere e conservare i log di accesso, in conformità alla normativa vigente e a quanto definito nel Titolo VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.
4. Nei log di cui al comma precedente sono contenuti i riferimenti temporali e gli identificativi delle postazioni e degli utenti che hanno effettuato l'accesso.
5. Con l'eccezione dei casi indicati nel presente articolo, sono vietate estensioni della RDA, temporanee o permanenti, effettuate tramite soluzioni VPN *gateway* o analoghi meccanismi di *tunnelling* per accedere da remoto alla RDA.
6. È vietato l'utilizzo di soluzioni VPN e meccanismi di *tunnelling* per eludere anche solo in parte i sistemi e le *policy* di sicurezza dell'Ateneo.

Art. 21 - Estensioni della Rete dati di Ateneo mediante VPN con modalità *Site to Site*

1. L'Amministratore della RDA realizza e gestisce estensioni della RDA effettuate mediante soluzioni VPN per consentire il corretto funzionamento delle soluzioni di tipo IaaS (*Infrastructure as a Service*) e PaaS (*Platform as a Service*) acquisite a supporto dei sistemi informativi di Ateneo.
2. L'estensione della RDA con VPN *site to site* deve avvenire utilizzando esclusivamente protocolli sicuri che garantiscano la confidenzialità e l'integrità delle informazioni veicolate su Internet.
3. Con l'eccezione dei casi indicati nel comma precedente, sono vietate estensioni della RDA, temporanee o permanenti, effettuate tramite soluzioni VPN *site to site* o analoghi meccanismi di *tunnelling*.

Art. 22 - Accesso per amministrazione remota ad *host* connessi alla Rete dati di Ateneo da reti esterne

1. L'accesso per amministrazione remota da reti esterne a sistemi informatici, telematici o apparati tecnologici connessi alla Rete dati di Ateneo, è consentito esclusivamente per la gestione e manutenzione di sistemi e apparecchiature.
2. Al fine di minimizzare i rischi informatici per RDA, gli *host* fisici o virtuali a cui è concessa la possibilità di connessione da reti esterne non possono essere superiori a due unità per ogni struttura.
3. Nei seguenti casi i referenti informatici di struttura possono implementare, ad uso proprio oppure di soggetti terzi incaricati, *host* di accesso remoto alla Rete dati di Ateneo:
   - particolari esigenze operative ravvisate dal Responsabile di Struttura;
   - specifiche clausole contrattuali con fornitori di servizi.
4. La funzione degli *host* di accesso remoto deve essere dichiarata all'Amministratore della RDA e da questi autorizzata secondo quanto previsto dell'art. 15, comma 2.
5. L'accesso agli *host* di accesso remoto deve essere soggetto ad autenticazione.
6. Le credenziali di accesso sono distinte per ogni soggetto autorizzato ad accedere agli *host* di accesso remoto.
7. Il canale di comunicazione verso gli *host* di accesso remoto deve essere cifrato e devono essere adottate tutte le politiche di sicurezza idonee per garantire confidenzialità e integrità della comunicazione.
8. I log di accesso raccolti presso gli *host* di accesso remoto devono essere conservati come specificato nel Titolo VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.
9. Il numero degli *host* di accesso remoto deve essere limitato allo stretto indispensabile.
10. Non sono consentite altre modalità di accesso remoto alla RDA.

Art. 23 - Modalità di utilizzo della Rete Dati di Ateneo

1. La RDA può essere utilizzata esclusivamente per gli scopi definiti dal presente regolamento, vale a dire come supporto alla ricerca, alla didattica, all'amministrazione e alle altre attività istituzionali dell'Università, nonché come strumento utile alla comunità dell'Ateneo; è vietato utilizzare la RDA per scopi incompatibili con quelli stabiliti ed in violazione della vigente normativa.
   In particolare, a titolo esemplificativo e non esaustivo, è vietato:
   a. accedere alla RDA per conseguire l'accesso non autorizzato a risorse di rete interne od esterne all'Università;
   b. fornire il servizio di connettività di rete a soggetti non autorizzati all'accesso alla RDA;
   c. usare false identità, l'anonimato o servirsi di risorse che consentono di restare anonimi. L'Amministratore di Sistema d'Ateneo e il Referente informatico si riservano la facoltà di impedire in qualsiasi momento l'accesso alla RDA da parte di utenti anonimi o non sufficientemente identificati o identificabili;
   d. trasferire o rendere disponibile materiale in violazione delle norme sulla proprietà intellettuale, mediante programmi di tipo *peer-to-peer* o altri strumenti;
   e. compiere azioni in violazione delle norme a tutela delle opere dell'ingegno, del diritto d'autore e del *software*;
   f. creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno. In particolare, è vietato la ricezione, la trasmissione o il possesso d'immagini pornografiche e pedo-pornografiche;
   g. trasmettere materiale commerciale e/o pubblicitario non richiesto (*spamming*), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;
   h. porre in essere attività che danneggiano l'immagine e il buon nome dell'Ateneo;
   i. utilizzare la RDA e i servizi da essa offerti a scopi commerciali e per propaganda politica o elettorale, tranne nei casi specificatamente autorizzati dal Rettore;
   j. utilizzare la rete dell'Ateneo per scopi che siano in contrasto con quanto previsto dalla AUP e dai regolamenti della rete GARR;
   k. svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distraggano risorse (persone, capacità, elaboratori), danneggino o restringano l'utilizzabilità o le prestazioni della RDA. È altresì vietato impedire o interferire o tentare di impedire in qualsiasi forma con i servizi offerti tramite la RDA agli altri Utenti e manomettere in qualsiasi modo le apparecchiature e le strutture informatiche ed elettroniche;
   l. violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (*software*, basi dati, ecc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete dati d'Ateneo, dei quali non si è destinatari specifici;
   m. distruggere, danneggiare, intercettare o accedere senza autorizzazione alla posta elettronica o ai dati di altri Utenti o di terzi;

n. usare, intercettare o diffondere *password* o codici d'accesso o chiavi crittografiche di altri Utenti o di terzi
o. commettere o tentare di commettere attività che violino la riservatezza di altri Utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;
p. è vietato installare modem configurati in *call-back*;
q. è vietato attivare accessi a Internet diversi da quello fornito dalla RDA, quali ad esempio tramite ADSL o servizi di telefonia mobile (WAP, UMTS, LTE, etc.)
r. è vietato l'accesso ai locali e agli armadi riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi senza l'autorizzazione dell'Amministratore della RDA;
s. è vietato cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione dell'Amministratore della RDA rilasciata tramite apposita registrazione sul portale web SOL;
t. è vietato utilizzare servizi o risorse di rete, collegare apparecchiature o servizi o *software* alla rete, diffondere *virus*, *malware* o altri programmi in un modo che interrompa o perturbi le attività di altre persone, utenti o i servizi disponibili sulla RDA.

Art. 24 - Modalità di utilizzo ed accesso a Internet

1. Il servizio di accesso a internet deve essere utilizzato a fini istituzionali, rispettando le regole di comportamento previste nel presente disciplinare e della AUP del Consortium GARR.
2. L'Università applicherà le restrizioni alla navigazione Web previste dalla vigente normativa e potrà altresì bloccare URL pericolosi per motivi di sicurezza come previsto dalle Misure minime di sicurezza ICT per le Pubbliche Amministrazioni[8] o applicare limitazioni alla navigazione Web per specifiche esigenze istituzionali. L'Università si riserva, altresì, la possibilità di applicare politiche di gestione della banda di trasmissione dati (*traffic shaping*) al fine di migliorare la fruibilità dei servizi legati alla ricerca, alla didattica e ai servizi istituzionali in generale.
3. È vietato accedere a siti che contengono foto o filmati di carattere pedo-pornografico, siti inibiti in base al decreto di "inibizione dei siti di gioco non autorizzati" allegato alla legge Finanziaria 2006 e pubblicati sul sito dell'Agenzia AAMS (http://www.aams.gov.it), siti che diffondono codici per l'utilizzo di *software* senza acquistarne la licenza e similari e quanto altro vietato dalla normativa vigente.
4. È vietato l'uso di servizi *web proxy* diversi da quelli istituzionali gestiti dall'Ateneo o per conto dell'Ateneo o autorizzati da quest'ultimo.

Art. 25 - Nomi a dominio

1. Il dominio DNS uninsubria.it e il dominio DNS uninsubria.eu sono gestiti dall'Amministratore della RDA negli interessi dell'Ateneo.
2. La gestione tecnica dei sottodomini di uninsubria.it ed uninsubria.eu è effettuata dall'Amministratore della RDA.
3. A ciascuna struttura può essere assegnato un sottodominio di III livello; i nomi dei calcolatori appartenenti alla struttura verranno registrati esclusivamente all'interno di tale sottodominio.
4. La registrazione di ulteriori nomi a dominio non inclusi nel dominio uninsubria.it o uninsubria.eu, a cui corrispondano *host* collegati alla rete dati di ateneo, deve sottostare alle norme dal Consortium GARR, in particolare quelle emanate dal NIC; la richiesta di registrazione di un nuovo nome a dominio andrà sottoposta al Responsabile dell'Area Sistemi Informativi, che, nel suo ruolo di *Access Port Administrator* nei confronti del Consortium GARR, provvederà a veicolarla al servizio NIC;
5. La richiesta di registrazione di un nuovo nome a dominio deve riportare il nominativo del responsabile amministrativo del dominio e del responsabile del DNS (eventualmente i nominativi possono coincidere).

Art. 26 - Modalità per l'erogazione di servizi sulla Rete dati di Ateneo

1. I soggetti autorizzati ad accedere alla RDA, possono erogare servizi tramite essa. Tali servizi dovranno essere conformi al presente disciplinare e ai regolamenti emanati dal Consortium GARR e dovranno essere dichiarati all'atto di richiedere l'accesso alla Rete come definito agli articoli 15 e 16.
2. A titolo puramente esemplificativo, ma non esaustivo, sono da considerarsi servizi erogati sulla rete: *http*, *https*, *ftp*, *samba*, *file-sharing*, *smtp*, *pop*, *imap*, *dns*, *dhcp*, *radius*, *ldap*, *proxy*, *vpn*, *streaming* audio e video etc.
3. I gestori di servizi erogati tramite la RDA devono provvedere alla raccolta e conservazione dei *log* di accesso in conformità alla vigente normativa ed a quanto definito nel TITOLO VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.
4. L'installazione di elaboratori *server* rispetta quanto descritto nell'art. 32.

Art. 27 - Monitoraggio e controlli

1. L'Amministratore della RDA ha facoltà di effettuare controlli, sulle attività svolte in rete nel rispetto dei diritti e delle libertà fondamentali degli utenti, ed in particolare dell'art. 4 dello Statuto dei Lavoratori, al fine di evitare usi impropri della rete o dei servizi di rete messi a disposizione dall'Ateneo.
2. I controlli di cui al comma precedente possono essere di natura preventiva o reattiva:
    a. Preventiva: utilizzando informazioni in modalità aggregata (non riconducibili direttamente all'utente) e non sistematica, per l'analisi del funzionamento della rete e per fini statistici;

   b. Reattiva: in caso di incidenti informatici o segnalazioni del Consortiun GARR potranno essere avviati controlli ex-post verso singoli *host* o gruppi di *host*.
3. Nell'effettuare detti controlli, l'Ateneo procederà in base al principio di gradualità. Pertanto, ove necessari, i controlli saranno effettuati inizialmente solo su dati aggregati riferiti alla generalità dell'Ateneo ovvero ad interi uffici, aree, settori o strutture e si concluderanno con un avviso generalizzato ovvero circoscritto all'ufficio, area, settore o struttura interessata.
4. Possono essere implementati filtri automatizzati sul traffico di rete volti a inibire l'accesso a siti *Web* o categorie di siti *Web* di palese natura non istituzionale o con contenuti pericolosi per la sicurezza della Rete Dati di Ateneo, tali filtri devono essere implementati senza tenere traccia, negli appositi file di *log*, degli *host* o degli utenti che hanno tentato di violare tali limitazioni.
5. L'Amministratore della RDA registra in appositi file di *log* i dati relativi all'accesso alla RDA e l'accesso a internet.
6. Nei *log* di cui al comma precedente non sono registrati i contenuti delle comunicazioni nè gli URL acceduti dai singoli *host* e dai singoli utenti.
7. L'Amministratore della RDA provvede alla raccolta e conservazione dei *log* di cui al comma 3 del presente articolo in conformità alla vigente normativa ed a quanto definito nel TITOLO VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.
8. Le informazioni raccolte nei *log* di cui al comma 3 del presente articolo possono essere messe a disposizione dell'autorità giudiziaria che può richiederne la conservazione per un periodo più lungo.
9. I controlli sulle attività svolte sulla RDA sono ammessi nei seguenti casi:
   a. nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
   b. su segnalazione dell'Autorità Giudiziaria;
   c. nel caso in cui i sistemi automatici di rilevamento statistico e diagnostico segnalino anomalie di funzionamento e/o di utilizzo della RDA.
10. Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illeciti o non conformi alla regolamentazione di Ateneo, l'Amministratore della RDA può intervenire valutando se:
    a. inviare avvisi collettivi, o ristretti a uno specifico gruppo di utenti, in cui verranno segnalati i comportamenti non corretti;
    b. inibire l'accesso a siti o categorie di siti di palese natura non istituzionale;
    c. inibire l'accesso alla Rete dell'Ateneo nelle modalità previste dal presente disciplinare;
    d. informare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, il Magnifico Rettore o il Direttore Generale, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni.

Titolo III - SISTEMA TELEFONICO DI ATENEO

Art. 28 - Telefonia fissa

1. L'Area Sistemi Informativi gestisce le infrastrutture di telefonia fissa dell'Ateneo.
2. Le utenze di telefonia fissa vengono richieste all'Area Sistemi Informativi tramite i SOL.
3. Il gestore delle infrastrutture telefoniche, raccoglie i *log* delle chiamate telefoniche effettuare da ciascun terminale fisso.
4. Nei *log* di cui al comma precedente le chiamate sono memorizzate in forma parzialmente anonimizzata occultando le ultime 3 cifre del numero chiamato.
5. La registrazione dei numeri chiamati è finalizzata esclusivamente:
    a. al controllo della spesa;
    b. all'identificazione di eventuali abusi o per essere messa a disposizione delle autorità di Pubblica Sicurezza nel caso ne venga fatta richiesta
6. I *log* delle chiamate vengono conservati in conformità alla normativa vigente. Per ulteriori dettagli sulle modalità di raccolta, gestione e conservazione dei *log* si fa riferimento alla specifica sezione Titolo VII 'Raccolta, gestione, conservazione ed utilizzo dei file di *log*'.

Art. 29 - Telefonia mobile

1. L'Ateneo acquisisce i servizi di telefonia mobile dagli operatori del settore.
2. Le utenze di telefonia mobile vengono richieste all'Area Sistemi Informativi tramite i SOL
3. Gli operatori telefonici raccolgono i dati del traffico telefonico e li conservano in conformità alla normativa vigente, per le finalità connesse al controllo della spesa.
4. Gli operatori forniscono all'Ateneo le registrazioni del traffico telefonico con le ultime 3 cifre del numero chiamato occultate.
5. L'Ateneo conserva tali registrazioni unicamente per i tempi correlati al controllo della spesa e conformemente alla normativa vigente.

Titolo IV - POSTAZIONI DI LAVORO

Art. 30 - Utilizzo degli elaboratori personali forniti dall'Ateneo

1. Ai fini del presente articolo sono considerati elaboratori personali i dispositivi di proprietà dell'Ateneo assegnati al personale, quali:
    a. *personal computer* da tavolo;
    b. *personal computer* portatili;
    c. *thin-client* e postazioni *diskless*;
    d. *tablet*, *smartphone* e dispositivi indossabili (es. *smart watch*, etc.)
2. Gli elaboratori personali e gli strumenti funzionalmente assimilabili sono strumenti di lavoro e il loro utilizzo deve essere finalizzato allo svolgimento delle attività professionali e istituzionali dell'Università.
3. Gli elaboratori personali sono predisposti con la necessaria dotazione di dispositivi (*hardware*) e programmi (*software*) tali da consentirne il corretto funzionamento e garantirne un adeguato livello di sicurezza.
4. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli elaboratori personali e da ridurre i rischi per la sicurezza del sistema informatico.
5. L'utilizzo degli elaboratori personali non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'Università o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.
6. Il *download* di file e/o la loro memorizzazione sugli elaboratori personali è legittimo solo se effettuato in relazione all'attività istituzionale.
7. Sugli elaboratori personali è altresì vietato:
    a. installare programmi tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché banche di dati che per la scelta o la disposizione del materiale costituiscano una creazione intellettuale dell'autore, se non in possesso delle relative licenze d'uso;
    b. installare programmi non inerenti l'attività lavorativa;
    c. installare programmi non preventivamente autorizzati i quali devono comunque essere comunicati al referente informatico di struttura;
    d. memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o comunque di natura illecita;
    e. installare *modem* oppure utilizzare dispositivi di telefonia mobile come punti di accesso alla RDA, se non preventivamente autorizzati dall'Amministratore della RDA.
8. Sugli elaboratori personali utilizzati per effettuare trattamenti di dati sensibili o giudiziari devono essere attuate le misure idonee di sicurezza conformi al principio di *accountability* previsto dall'art. 32 del GDPR, in particolare devo essere previsti:
    a. la pseudonimizzazione e la cifratura dei dati personali;

b. misure di sicurezza idonee a garantire la riservatezza, l'integrità, la disponibilità dei dati trattati, nonché e la resilienza dei sistemi e dei servizi utilizzati per il loro trattamento;
c. idonee procedure di *disaster recovery* al fine di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso guasti fisici, logici dei sistemi nonché di incidenti informatici più in generale;
d. adottare adeguate procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento dei dati effettuato.

9. Al fine di evitare l'utilizzo della postazione personale da terzi non autorizzati, l'accesso alla postazione lavorativa deve essere protetto da apposite credenziali di accesso, l'utente è tenuto a bloccare o spegnere il *personal computer* in caso di sospensione o termine dell'attività lavorativa. Le stazioni di lavoro, da tavolo o portatili, o gli strumenti comunque funzionalmente assimilabili, messe a disposizione dall'Ateneo, non devono essere lasciati incustoditi; al termine dell'orario di servizio, i computer devono essere spenti prima di lasciare gli uffici; in caso di allontanamento anche temporaneo, al fine di evitare che persone estranee effettuino accessi non consentiti, l'Utente deve attivare il salvaschermo con sblocco tramite *password*.
10. Per la disciplina riguardante l'utilizzo delle credenziali e la segretezza e tutela delle *password* devono essere adottate delle misure di sicurezza idonee e adeguate nel rispetto dell'art. 32 del GDPR.

Art. 31 - Utilizzo dei terminali telefonici dell'Ateneo

1. I terminali telefonici fissi e mobili messi a disposizione dell'Ateneo, sono strumenti di lavoro e il loro utilizzo deve essere finalizzato allo svolgimento delle attività professionali e istituzionali dell'Università.
2. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza del sistema telefonico.
3. L'utilizzo dei terminali telefonici non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'Università o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.
4. Sui terminali telefonici mobili forniti dall'Ateneo è vietata l'installazione di applicazioni o *software* non strettamente correlato a finalità lavorative ed istituzionali ed in ogni caso applicazioni o software di cui non sia regolarmente detenuta la licenza d'utilizzo.

Titolo V - ELABORATORI *SERVER*

Art. 32 - Installazione e utilizzo degli elaboratori *server*

1. Gli elaboratori *server* sono *host* connessi alla RDA che erogano servizi destinati esclusivamente alle finalità istituzionali dell'Università.
2. I Responsabili di struttura vigilano affinché i *server* operanti presso la propria struttura siano utilizzati correttamente e mantenuti a un adeguato livello di sicurezza dai Referenti informatici di struttura di cui all'art. 11.
3. L'installazione di applicazioni e l'attivazione di servizi su elaboratori *server* connessi alla RDA è legittimo solo se effettuato in relazione con l'attività istituzionale.
4. Sui *server* è vietato:
    a. installare programmi tutelati ai sensi della convenzione sulla protezione delle opere letterarie e artistiche, nonché banche di dati che per la scelta o la disposizione del materiale costituiscano una creazione intellettuale dell'autore, se non in possesso delle relative licenze d'uso;
    b. installare programmi non inerenti l'attività lavorativa;
    c. memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o di natura comunque illecita;
    d. utilizzare dispositivi esterni personali per la memorizzazione di dati;
    e. installare oppure utilizzare dispositivi di telefonia mobile come punti di accesso alla RDA, se non preventivamente autorizzati dall'Amministratore della RDA.
5. Sugli elaboratori *server* utilizzati per effettuare trattamenti di dati sensibili o giudiziari devono essere attuate le misure di sicurezza idonee ed adeguate ai sensi dell'art. 32 del GDPR.
6. Devono essere raccolti e conservati i *log* di accesso con privilegi di amministrazione in conformità alla vigente normativa e a quanto definito nel TITOLO VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG.

Art. 33 - Gestione degli elaboratori *server*

1. Gli aggiornamenti relativi alla sicurezza rilasciati dai produttori dei sistemi operativi e degli applicativi installati sugli elaboratori *server* devono essere installati tempestivamente.
2. Le *password* per l'accesso ai *server* con privilegi di amministrazione sono:
    a. note esclusivamente ai Referenti informatici di struttura che si occupano della gestione operativa;
    b. conservate in luogo sicuro e accessibile al Responsabile di struttura;
    c. sufficientemente complesse (lunghezza non inferiore a 12 caratteri, contenenti caratteri minuscoli e maiuscoli, contenenti caratteri speciali, non composte

esclusivamente da parole esistenti nei vocabolari, non contenenti riferimenti anagrafici del titolare dell'utenza, etc)

d. devono essere cambiate con frequenza non inferiore a 90 giorni con nuove *password* diverse da quelle utilizzate in precedenza;
e. usate esclusivamente per amministrare gli elaboratori *server*.

3. Al fine di tracciare correttamente l'esecuzione delle operazioni di gestione operativa gli amministratori di sistema devono usare credenziali personali per l'accesso ai *server* riconducili a una persona fisica in modo univoco.
4. Le stesse credenziali con privilegi di amministrazione dei *server* non possono essere assegnate a persone diverse neanche in tempi diversi, con l'esclusiva eccezione di quei sistemi che ammettono un solo livello di *userid* per l'amministrazione.
5. Se il *server* ospita un sistema di autenticazione oppure *database* contenenti le credenziali di accesso degli utenti, le *password* devono essere memorizzate in modalità cifrata.
6. L'accesso da remoto ai *server* per finalità di amministrazione deve avvenite tramite connessioni di rete protette e utilizzando applicazioni e canali di comunicazioni sicuri.
7. Effettuare con regolarità la ricerca di eventuali vulnerabilità sui sistemi *server* (sia per il sistema operativo che per le applicazioni installate) e provvedere tempestivamente alla loro risoluzione adeguando le configurazioni e applicando ove disponili le *patch* di sicurezza, come previsto dalla Misure minime di sicurezza ICT per le Pubbliche Amministrazioni.

Titolo VI - SERVIZI DI POSTA ELETTRONICA

Art. 34 - Soggetti titolari di una casella di posta elettronica di Ateneo

1. L'Università degli Studi dell'Insubria, tramite l'Area Sistemi Informativi, rende disponibile un servizio istituzionale di posta elettronica.
2. Al Personale docente, ricercatore e tecnico amministrativo, borsisti, assegnisti, stagisti o altri soggetti titolari di contratti di ricerca o di didattica, ai professori Emeriti, professori Onorari, professori Senior e ricercatori Senior, ai collaboratori e consulenti titolari di un contratto con l'Ateneo, è associato un indirizzo di posta elettronica afferente al dominio *@uninsubria.it*
3. Agli studenti registrati a corsi di studio magistrale non ciclo unico, immatricolati e iscritti a corsi di studio, iscritti a master e corsi di perfezionamento, è associato un indirizzo di posta elettronica afferente al dominio *@studenti.uninsubria.it*
4. Agli studenti iscritti a un corso di dottorato o di specializzazione oltre all'indirizzo *@studenti.uninsubria.it* è associato un secondo indirizzo afferente al dominio *uninsubria.it*
5. I casi di omonimia sono risolti mediante apposizione di un suffisso numerico incrementale al termine della stringa nome.cognome nel caso di dominio *uninsubria.it* e n.cognome nel caso di dominio *studenti.uninsubria.it.*
6. Al fine di agevolare la comunicazione istituzionale e favorire la circolazione delle informazioni, sono altresì fornite caselle di posta elettronica per AOO/UOR, codificate nel formato base *aoo/uor@uninsubria.it*, e per cariche istituzionali codificate nel formato base *carica@uninsubria.it* oppure *carica.aoo@uninsubria.it.*
7. Le comunicazioni ufficiali e istituzionali da parte dell'Ateneo sono inviate esclusivamente all'indirizzo di posta istituzionale.

Art. 35 - Ambito di utilizzo del servizio di posta elettronica di Ateneo

1. Il servizio di posta elettronica è fornito in funzione dell'attività didattica, dell'attività di ricerca, dell'attività amministrativa e delle altre attività strumentali o correlate ai fini istituzionali dell'Università.
2. Le comunicazioni ufficiali e istituzionali dell'Ateneo destinate ai soggetti titolari di una Identità digitale di Ateneo, sono inviate esclusivamente agli indirizzi istituzionali di posta elettronica.
3. È opportuno che ogni persona consulti regolarmente la propria casella istituzionale di posta elettronica.
4. Allo scopo di conseguire un più efficace impiego del servizio e nel contempo non sovraccaricare i relativi sistemi di sicurezza, è opportuno eliminare dalla casella istituzionale di posta elettronica i messaggi non necessari e i relativi allegati.
5. Non è consentito utilizzare la posta elettronica per diffondere, anche tramite collegamenti ipertestuali o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice eseguibile, ecc.), messaggi che contengano o rimandino a:
   - pubblicità non istituzionale, manifesta od occulta;

- partecipazione a *forum* e/o dibattiti se non per motivi istituzionali, per diffondere notizie non veritiere o quanto altro che abbia contenuto offensivo e discriminatorio;
- comunicazioni commerciali private;
- materiale pornografico o che possa comportare una violazione della Legge 6 febbraio 2006, n. 38, *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*;
- materiale discriminante o lesivo in relazione a razza, sesso, religione;
- materiale che violi la normativa in materia di protezione dei dati personali;
- contenuti o materiali che violino i diritti d'autore di terzi;
- materiale contenente codici sorgenti malevoli (ad es., malware o virus informatici);
- altri contenuti illegali;
- catene telematiche.

6. Non è consentito usare l'indirizzo di posta elettronica istituzionale per accedere ai profili personali di *social network*, o di altre applicazioni o servizi *on line*.
7. È necessario prestare la massima attenzione alla posta elettronica ricevuta. Specificamente:
   - Nel caso di mittenti sconosciuti o messaggi insoliti o contenenti allegati sospetti, per non correre il rischio di essere infettati da *malware* occorrerà cancellare i messaggi senza aprirli e nel dubbio informare gli Amministratori di Sistema per ogni necessaria verifica inviando una comunicazione a assistenza.tecnica@uninsubria.it.
   - È obbligatorio controllare i File "*attachments*" (allegati) di posta elettronica prima del loro utilizzo ed è vivamente sconsigliato il *download* di *file* eseguibili o documenti da siti *Web* o *ftp* non conosciuti.
8. La conservazione dei dati relativi all'uso degli strumenti elettronici e delle *e-mail* avverrà secondo principi di necessità, pertinenza e non eccedenza, nei limiti previsti dalle vigenti disposizioni di legge ove applicabili da valutarsi in relazione:
   - ad esigenze connesse al valore o alla natura contrattuale dei messaggi di posta elettronica per i quali vi sia un obbligo di conservazione;
   - ad esigenze aziendali tecniche o di sicurezza;
   - all'indispensabilità del dato rispetto all'esercizio di un diritto o alla difesa in sede giudiziaria;
   - all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.
9. In caso di assenze programmate o prevedibili è opportuno che il personale dell'Ateneo attivi la funzione di risposta automatica per comunicare ai mittenti eventuali contatti alternativi.
10. In caso di assenza prolungata o improvvisa, è opportuno che il singolo dipendente si adoperi per consentire all'Ateneo la corretta ricezione e gestione dei messaggi

pertinenti all'attività istituzionale eventualmente recapitati nella propria casella di posta elettronica. Qualora tale accorgimento non sia posto in essere dal dipendente o, a tutela del buon andamento e dell'efficienza dell'attività istituzionale, si configuri la necessità di accedere ai messaggi giacenti nella casella di posta elettronica del dipendente, l'Ateneo si riserva la facoltà di attivare le misure tecniche atte a consentire al Responsabile della AOO/UOR di appartenenza del dipendente di accedere alla casella di posta attribuendo temporaneamente a quest'ultimo diritti di delega. Di tale attività deve essere redatto apposito verbale e deve essere informato l'utente interessato alla prima occasione utile.

11. L'utilizzo degli indirizzi di posta elettronica *@unininsubria.it* e *@studenti.uninsubria.it*, costituisce "trattamento dei dati personali" pertanto, da conformarsi alle disposizioni del GDPR e del D.Lgs. 196/2003 e successive modifiche (D.lgs. 10 agosto 2018, n. 101).

Art. 36 - Accesso al servizio di posta elettronica

1. L'accesso al servizio di posta elettronica di Ateneo avviene mediante l'utilizzo delle credenziali associate alla propria identità digitale, costituite da *nome utente* e *password*.
2. La *password* ha le seguenti caratteristiche
    a. Lunghezza minima: Minimo 8 caratteri (sarebbe meglio utilizzare *password* complesse di 15 o più caratteri);
    b. Unicità: il sistema non consente di impostare una *password* uguale a quelle utilizzate in precedenza.
    c. Complessità: la *password* deve soddisfare almeno tre dei seguenti quattro criteri
    d. Contenere almeno: (i) un carattere maiuscolo dell'alfabeto Inglese (A-Z); (ii) un carattere minuscolo dell'alfabeto inglese (a-z); (iii) un numero (0-9); (iv) un carattere speciale (es. !, $, #, %)
    e. Non può contenere lo *username*, né il nome o il cognome, se questi sono più lunghi di due caratteri.
    f. Deve essere sostituita ogni tre mesi.
3. L'accesso alla casella *email* istituzionale deve avvenire esclusivamente tramite la pagina *web* del servizio Office 365 o utilizzando client o APP per l'accesso al sistema di posta elettronica, che siano sicure e mantenute aggiornate all'ultima versione sicura rilasciata dal produttore.
4. Le caselle di posta elettronica di cui al punto 34 comma 10 sono create come caselle con delega, ossia caselle *email* non riferibili ad una persona fisica, a cui possono accedere più utenti utilizzando le credenziali di accesso riferite alla propria identità digitale personale.
5. I soggetti titolari delle caselle di posta elettronica istituzionali sono responsabili del corretto utilizzo delle stesse e sono tenuti a conservare nella massima segretezza le Credenziali di Autenticazione, così come qualsiasi altra informazione legata al processo di autenticazione. In particolare, non bisogna:
    a. rivelare o condividere la *password* con nessuno, compresi colleghi di lavoro, familiari e amici;

b. digitare la *password* davanti a terzi che potrebbero osservare l'operazione;
c. scrivere la *password* in un messaggio di posta elettronica o su supporti cartacei conservati in ufficio;
d. archiviare la *password* su un qualsiasi strumento elettronico, incluso il telefono cellulare, senza utilizzare un sistema di crittografia.

La *password* deve essere immediatamente sostituita, dandone comunicazione agli Amministratori di Sistema dell'Ateneo, nel caso si sospetti che la stessa abbia perso la segretezza.

Art. 37 - Ciclo di vita delle caselle di posta elettronica

1. Le modalità di attivazione e disattivazione delle caselle di posta elettronica sono definite all'art. 7 relativo ai servizi associati alle identità digitali di Ateneo.
2. L'accesso alle caselle di posta elettronica con delega è disabilitato contestualmente alla revoca dei permessi di accesso dell'ultimo delegato attivo e i messaggi in esse contenuti sono cancellati definitivamente dopo 30 giorni.
3. Durante il periodo di utilizzo il titolare di una casella con delega è tenuto a comunicare tempestivamente all'Area Sistemi Informativi eventuali variazioni dei permessi di accesso dei delegati.
4. Le comunicazioni relative alla disattivazione delle caselle di posta elettronica sono inviate solo all'indirizzo istituzionale con un preavviso di almeno 60 giorni.

Art. 38 - Liste di distribuzione

1. L'utilizzo delle liste di distribuzione costituisce "trattamento dei dati personali" e deve, dunque, svolgersi nell'ambito delle attività istituzionali dell'ente e nel rispetto delle disposizioni previste dal GDPR e dal D.Lgs. 196/2003 e successive modifiche (D.lgs. 10 agosto 2018, n. 101).
2. Le liste di distribuzione di Ateneo costituiscono uno strumento volto ad agevolare lo scambio di informazioni tra gli utenti dell'Ateneo nello svolgimento delle proprie attività istituzionali. Non è pertanto ammesso l'invio di messaggi non attinenti a tali finalità, o quello relativo ad informazioni, comunicazioni e note di carattere propagandistico, politico (qualora il tema esuli dal contesto di specifico interesse scientifico dell'Ateneo), commerciale, pubblicitario, personale o qualsivoglia altro fine non correlato a un interesse istituzionale dell'Ateneo nel suo complesso. I messaggi di posta elettronica non devono avere contenuto offensivo, calunnioso, diffamatorio, né essere contrari alla legge, all'ordine pubblico, al buon costume.
   La pubblicità di liste di distribuzione sui sistemi informativi d'Ateneo non ne legittima l'utilizzo per finalità contrastanti con il presente Regolamento o con la normativa vigente in materia di tutela dei dati personali.

Art. 39 - Liste di distribuzione istituzionali

1. In base al principio per cui i messaggi diffusi tramite *mailing list* devono rispettare l'attinenza soggettiva o per materia rispetto ai destinatari, sono disponibili liste generali

di distribuzione (di seguito denominate liste istituzionali), comprendenti gli utenti suddivisi per tipologia.
2. L'Ateneo può implementare meccanismi di moderazione sulle liste di distribuzione.
3. La creazione di liste di distribuzione istituzionali, deve tenere conto di criteri secondo i quali il numero dei componenti di una lista ed i relativi utilizzatori (mittenti) deve essere significativo, nonché della strategicità e/o criticità delle finalità correlate alla lista stessa.
4. Per ogni lista deve essere definito il sistema informativo (banca dati) autoritativo per il suo popolamento nel caso di liste automatizzate, mentre per le liste non automatizzate (i cui membri vengono gestiti da operatore) deve essere identificata l'Unità organizzativa responsabile (UOR) incaricata di comunicare all'Area Sistemi Informativi gli aggiornamenti della lista stesa.
5. È competenza dell'Area Sistemi Informativi la creazione e la gestione informatizzata delle liste di distribuzione istituzionali.
6. Le liste di distribuzione istituzionali possono avere le seguenti caratteristiche:
    a. Liste Moderate: l'inoltro alla lista di un messaggio deve essere preventivamente approvato dal suo moderatore;
    b. Liste Moderate con *by-pass*: hanno le stesse caratteristiche delle Liste Moderate ma solo alcuni utenti possono inoltrare messaggi senza l'intervento del moderatore;
    c. Liste non Moderate: l'inoltro alla lista avviene senza filtri né intermediari.
7. Alcune liste istituzionali, su indicazione del Magnifico Rettore o del Direttore Generale possono essere Moderate. Per particolari soggetti (es. Rettore, Direttore Generale, Ufficio Personale…) è possibile richiedere al Direttore Generale il *by-pass* per l'inoltro dei messaggi direttamente alla lista senza l'intervento del Moderatore.
8. Ad alcune liste istituzionali, su indicazione del Magnifico Rettore o del Direttore Generale, possono essere applicare restrizioni all'invio, ossia solo gli utenti autorizzati potranno inviare messaggi.
9. Le liste di distribuzione istituzionali possono essere configurate per ricevere messaggi solo da indirizzi appartenenti all'Ateneo e non da indirizzi esterni.
10. La responsabilità in merito al contenuto dei messaggi, è comunque integralmente a carico dei soggetti autori e/o diffusori dei messaggi stessi.

Art. 40 - Monitoraggi e controlli

1. L'utilizzo della *Suite Office 365* (Sistema Informatico) nel suo complesso, la quale racchiude fra gli altri il servizio di posta elettronica, potrà essere soggetto ad accessi e controlli, anche tramite applicativi, gestionali e funzionalità che consentono la raccolta e il trattamento dei dati personali riferiti o riferibili ai titolari di una casella di posta elettronica, nel rispetto dei principi di finalità, liceità, necessità, pertinenza e non eccedenza e, in ogni caso, in modo tale da evitare ingiustificate interferenze con i diritti e le libertà fondamentali, escludendosi sin da ora controlli continuativi, costanti, prolungati e/o discriminatori.

2. I controlli potranno essere effettuati, tra l'altro, per verificare la corretta applicazione del presente Regolamento, per garantire la sicurezza del Sistema Informatico, per motivi tecnici e/o interventi di manutenzione (quali, aggiornamento/sostituzione/ implementazione di programmi, manutenzione *hardware*, etc.), per garantire la sicurezza del lavoro e per la tutela del patrimonio aziendale connessi all'utilizzo dei dispositivi.
3. Ai sensi del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007, n. 13, recante le "Linee Guida per posta elettronica e internet" si precisa che i controlli potranno essere effettuati dall'Area Sistemi Informativi. In ogni caso, saranno autorizzati ad accedere e a trattare i dati personali presenti nel Sistema Informatico solamente i soggetti nominati quali autorizzati, ai sensi del Regolamento UE 679/2016 e del D. Lgs. 196/2003. Gli esiti di tali controlli potranno inoltre essere comunicati all'Ateneo, agli enti pubblici, alle autorità giudiziarie e di polizia, nonché a consulenti - ivi inclusi quelli legali e fiscali - per ogni conseguente determinazione.
4. Nell'effettuare detti controlli, l'Ateneo procederà in base al principio di gradualità. Pertanto, ove necessari, i controlli saranno effettuati inizialmente solo su dati aggregati riferiti alla generalità dell'Ateneo ovvero ad interi uffici, aree, settori o strutture e si concluderanno con un avviso generalizzato ovvero circoscritto all'ufficio, area, settore o struttura interessata, contenente tra l'altro l'invito di attenersi scrupolosamente al presente Regolamento. Qualora si dovessero riscontrare reiterate violazioni del presente Regolamento, indizi di commissione di gravi abusi o di illeciti e l'anomalia inizialmente rilevata dovesse persistere, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale e con il coinvolgimento di consulenti legali esterni appositamente nominati ai sensi della legge 7 dicembre 2000, n. 397 recante "Disposizioni in materia di indagini difensive" e tecnici informatici autorizzati.
5. In ogni caso, le modalità di effettuazione dei controlli sono state determinate dall'Ateneo sulla base di una valutazione, condotta alla luce delle attuali conoscenze tecnologiche e dei dispositivi concretamente utilizzati, volta a determinare i concreti rischi per la sicurezza dei dati personali dagli stessi derivanti e a individuare le misure di sicurezza e i meccanismi necessari a ridurre al minimo tali rischi.
6. In ogni caso, l'Ateneo non effettua attività di controllo sistematico, quali, ad esempio:
   - la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
   - la lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
   - l'analisi occulta di computer portatili affidati in uso.
7. L'Area Sistemi Informativi per motivi tecnici e di sicurezza e in particolare per prevenire malfunzionamenti, effettua una registrazione delle componenti di traffico (*file di log*) riferiti alla posta elettronica e degli accessi alla Rete dell'Ateneo sia con elaboratori connessi alla rete cablata sia in modalità *Wireless*.

Art. 41 - Modalità di gestione degli incidenti

1. Nel caso dei seguenti eventi l'accesso ai servizi di posta elettronica può essere totalmente o parzialmente limitato dall'Ateneo, senza necessità di assenso da parte dell'utente e anche senza preavviso:
   a) quando richiesto dalla legge e in conformità a essa;
   b) in caso di comprovati motivi che facciano ritenere la violazione delle presenti regole e delle disposizioni di legge vigenti;
   c) in casi eccezionali, quando richiesto, per esigenze operative critiche e improcrastinabili.

Titolo VII - RACCOLTA GESTIONE E CONSERVAZIONE DEI LOG

Art. 42 - Ambito di applicazione

1. La maggior parte dei sistemi telematici genera *file* di *log*, ovvero registri informatizzati, ove viene tenuta traccia degli eventi di sistema significativi unitamente alla data e all'orario in cui si sono manifestati.
2. Il monitoraggio e l'analisi dei *file* di *log* consentono di verificare il corretto funzionamento dei sistemi e di diagnosticare eventuali anomalie o abusi dei servizi erogati.
3. La raccolta e conservazione dei *log* è, anche ai sensi dell'art.132 del D. Lgs. 30 giugno 2003, n. 196 e s.m.i, un obbligo di legge al fine di coadiuvare le autorità di Pubblica Sicurezza per l'indagine e la repressione dei reati informatici.
4. Qualunque struttura dell'Ateneo che, per obblighi di legge o di regolamenti, è tenuta al mantenimento dei *log*, deve trattare tali dati conformemente alla normativa vigente. A titolo esemplificativo ma non esaustivo, si ricorda che devono essere raccolti i *log* per:
    a. i servizi telefonici accessibili al pubblico
    b. il servizio di accesso a internet
    c. il servizio di posta elettronica
    d. l'accesso con privilegi di amministratore ai sistemi che trattano dati o banche dati classificate come sensibili o giudiziarie ai sensi del D. Lgs. 30 giugno 2003, n. 196 e s.m.i.
5. Si configurano principalmente due ambiti di raccolta con finalità, modalità e prerogative distinte:
    a. raccolta *log* finalizzata alla gestione ordinaria
    b. raccolta e conservazione per finalità di accertamento e repressione dei reati.

Art. 43 - Normativa di riferimento

1. La raccolta, consultazione, conservazione e comunicazione a terzi dei file di *log* sui sistemi dell'Università degli Studi dell'Insubria deve avvenire nel rigoroso rispetto della normativa nazionale e comunitaria vigente, in particolare:
    - D. Lgs. 30 giugno 2003, n. 196 *Codice della Privacy* come modificato dal D.lgs. 10 agosto 2018, n. 101.
    - Regolamento 679/2016/EU - *GDPR*
    - Direttiva 2006/24/EU riguardante la conservazione dei dati generati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico e di reti pubbliche di comunicazione.
    - D. Lgs 30 maggio 2008, n. 109 riguardante l'attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al

pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.
- Delibera 1° marzo 2007, n. 131 del Garante per la Protezione dei dati personali riguardante le linee guida del Garante per posta elettronica e internet.
- Provvedimento 17 gennaio 2008 del Garante per Protezione dei Dati Personali riguardante la sicurezza dei dati di traffico telefonico e telematico.
- Provvedimento 27 novembre 2008 del Garante per Protezione dei Dati Personali riguardante misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
- Legge 20 novembre 2017, n. 167 Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge europea 2017, art. 27 Termini di conservazione dei dati di traffico telefonico e telematico.

Art. 44 - Tipologia dei dati di *log* raccolti

1. I dati raccolti dai sistemi telematici, per i quali si applica l'obbligo di raccolta e conservazione per prevenzione dei reati informatici, devono essere raccolti in conformità alla normativa vigente, a titolo esemplificativo ma non esaustivo si citano i seguenti esempi:
    a. servizi di telefonia: numero telefonico chiamante e chiamato, recapito del chiamante se afferente ai sistemi telefonici gestiti dall'Ateneo, data, orario e durata della comunicazione;
    b. servizi di accesso a internet: dati necessari a identificare l'utilizzatore di un indirizzo IP appartenente alla Rete dati di Ateneo, data e orario di assegnazione dell'indirizzo IP all'utenza e durata di validità dello stesso ed eventualmente l'indirizzo fisico della scheda di rete (*MAC address*).
    c. servizi di posta elettronica: indirizzi di posta elettronica del mittente e dei destinatari di una comunicazione, data e orario della comunicazione; identificativo utente del possessore della casella di posta elettronica mittente o destinataria e la data e orario di *log in* e *log out* al servizio di posta elettronica nel caso afferisca a servizi di posta elettronica appartenenti all'Università.
    d. Accesso con privilegi di amministratore di sistema ad elaboratori che trattino dati classificati ai sensi del GDPR e del D. Lgs. 30 giugno 2003, n. 196 come modificato dal D.lgs. 10 agosto 2018, n. 101: *log in* e *log out* accessi per privilegi di amministrazione, corredati di data, orario e identificativo dell'utente che ha effettuato l'attività.

Art. 45 - Modalità di raccolta e conservazione

1. I dati di *log* raccolti nell'ambito delle finalità di *gestione ordinaria* di cui all'art. 39, comma 5a:

a. devono essere soggetti a misure di sicurezza tecniche ed organizzative idonee ad impedirne l'accesso a persone non autorizzate;
b. devono essere conservati per il tempo strettamente necessario alla finalità a cui sono destinati (ad esempio il monitoraggio e la gestione dei servizi) e comunque non superiore a sei mesi; terminati i tempi di conservazione prefissati i dati devono essere cancellati dai sistemi che li ospitano compresi eventuali supporti di *backup*;
c. devono essere formati in modo tale da raccogliere solo i dati strettamente necessari ed in ogni caso evitando di registrare informazioni in violazione delle direttive del Garante Privacy specificatamente ai servizi accesso a internet ed ai servizi di posta elettronica;
d. non possono essere comunicati a terzi.

2. I dati di *log* raccolti con *finalità di repressione dei reati* di cui all'art. 39, comma 5b, devono essere raccolti in conformità alla normativa vigente, a titolo esemplificativo ma non esaustivo si ricorda che:
   a. i *file* di *log* così raccolti devono essere utilizzati esclusivamente per le finalità di accertamento e repressione dei reati;
   b. i *file* di *log* raccolti devono essere soggetti a misure di sicurezza tecniche ed organizzative idonee ad impedirne l'accesso a persone non autorizzate (ad esempio con *firewall*, protezione degli spazi di memorizzazione tramite *password* adeguate, crittografia);
   c. i *file* di *log* con finalità di repressione dei reati devono essere conservati tramite sistemi informatici fisicamente distinti da quelli per la memorizzazione dei *log* per la gestione ordinaria, e deve essere redatta apposita documentazione atta a descrivere i sistemi preposti e coinvolti;
   d. devono essere nominati i soggetti autorizzati ad accedere a tali *file* di *log*, nonché devono essere adottati strumenti e procedure atte ad assicurare adeguato controllo sulle attività svolte da ciascun incaricato;
   e. i *file* di *log* devono essere conservati in modo tale da impedire la loro alterazione (ad esempio con meccanismi di firma digitale del *file* oppure di *hashing* di controllo);
   f. i *file* di *log* devono essere protetti con misure tecniche ed organizzative idonee ad evitare la loro perdita accidentale (ad esempio con sistemi di *back-up*), garantendone la disponibilità entro 7 giorni anche in caso di danneggiamento dei dispositivi preposti alla conservazione;
   g. i *file* di *log* devono riportare gli estremi temporali corretti della registrazione degli eventi, devono essere adottati meccanismi per il mantenimento di un corretto allineamento dell'orologio di sistema, a tal fine è obbligatario sincronizzare i dispositivi che registrano i *log* mediante protocollo NTP con i *time server* dell'Ateneo;
   h. il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del Decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla Legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi.

i. i *file* di *log* non contemplati nel comma 2.h devono essere conservati in conformità alla normativa vigente per un periodo non superiore a 24 mesi; terminati i tempi di conservazione prefissati i dati devono essere cancellati dai sistemi che li ospitano compresi eventuali supporti di *backup*.

3. Le strutture che raccolgono e conservano i log di cui sopra, dovranno redigere apposito documento in cui si definiscono le modalità di conservazione dei dati, le politiche di *backup* e relativi responsabili, nonché le procedure di verifica di integrità dei log e ripristino dei file di *backup*.

Art. 46 - Utilizzo e comunicazione a terzi dei dati raccolti

1. I dati raccolti dai sistemi telematici per finalità di giustizia possono essere messi a disposizione dell'autorità giudiziaria, a fronte di specifico decreto di esibizione motivato del Pubblico Ministero (art.132 comma 3 del D. Lgs. 30 giugno 2003, n. 196 come modificato dal D.lgs. 10 agosto 2018, n. 101), il quale può richiedere la non cancellazione e la conservazione per un periodo più lungo.
2. Le informazioni desumibili dai *file* di *log* di ordinaria gestione, possono essere utilizzate dall'Ateneo nella modalità aggregata (non riconducibile direttamente all'utente) per l'analisi del funzionamento dei sistemi e per fini statistici.
3. Grazie alle informazioni contenute nei *file* di *log* di ordinaria gestione, per esigenze organizzative, produttive e di sicurezza l'Università può effettuare, altresì, controlli di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, settori o gruppi di utenti.
4. In caso di incidenti informatici, potranno essere avviati controlli mirati ex-post su singoli o gruppi di *host* facendo uso dei *log* per finalità di ordinaria gestione.
5. I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi nei seguenti casi:
    a. nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
    b. su segnalazione dell'Autorità Giudiziaria;
    c. in caso di verifiche più specifiche e puntuali, anche su base individuale e con il coinvolgimento di consulenti legali esterni appositamente nominati ai sensi della legge 7 dicembre 2000, n. 397 recante "Disposizioni in materia di indagini difensive" e tecnici informatici autorizzati.
    d. nel caso in cui i sistemi automatici di rilevamento statistico e diagnostico segnalino anomalie di funzionamento e/o di utilizzo della RDA.
6. In ogni caso i dati raccolti nei *file* di *log* o le informazioni ad esse collegate, non potranno essere comunicate a terzi se non alle autorità di Pubblica Sicurezza e a fronte di loro formale richiesta.

Art. 47 - Informativa agli utenti sulle modalità, tipologia ed utilizzo dei dati raccolti

1. Le strutture che raccolgono i dati, in virtù di quanto espresso nella normativa di cui all'art. 40, hanno l'obbligo di presentare all'interessato l'informativa relativa alla gestione dei dati di traffico.
2. Ai sensi dell'art. 13 del GDPR, tale comunicazione deve contenere almeno le seguenti informazioni:
    a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
    b. i dati di contatto del responsabile della protezione dei dati, ove applicabile;
    c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
    d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del GDPR, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
    e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
    f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo
    g. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
    h. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
    i. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del GDPR, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
    j. il diritto di proporre reclamo a un'autorità di controllo;
    k. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
    l. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
    m. le categorie di soggetti che detengono i *log file*;
    n. i soggetti o le categorie di soggetti ai quali i file di log possono essere comunicati o i soggetti esterni che possono venirne a conoscenza;
    o. natura e contenuto informativo dei *log* conservati (ad esempio se contengono dati personali o sensibili).

Titolo VIII – GESTIONE DEGLI INCIDENTI INFORMATICI CON CONSEGUENTE DATA BREACH

Art. 48 - Definizione di Data Breach

L'articolo 4 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, sancisce che una violazione dei dati personali ("*Data Breach*") è "una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
Il Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art.29 della Direttiva Europea 95/46, con le linee guida WP250, ha meglio precisato che i *Data Breach* sono classificabili in tre macro-categorie:

1. "*Confidentiality Breach*", quando vi è un accesso accidentale o abusivo a Dati personali;
2. "*Availability Breach*", quando vi è una perdita o distruzione accidentale o non autorizzata del Dato personale;
3. "*Integrity Breach*", quando vi è un'alterazione accidentale o non autorizzata del Dato personale

Gli eventi che possono causare un *Data Breach* sono così raggruppati nell'articolo 4(12) del GDPR sulla base delle linee guida ENISA:

- *Unauthorized Access*: accesso ai dati da parte di soggetti (interni o esterni) non aventi diritto;
- *Loss*: indisponibilità temporanea dei dati;
- *Destructio*n: indisponibilità irreversibile dei dati;
- *Transmission*: comunicazione (fortuita o intenzionale) dei dati verso destinatari non autorizzati;
- *Alteration or Modification*: modifica impropria (accidentale o intenzionale) dei dati;
- *Disclosure*: divulgazione impropria di informazioni riservate.

L'Ateno si è dotato di procedure per la gestione dei Data Breach descritte nell'Allegato E.

Art. 49 - Notifiche correlate ad un *Data Breach*

1. Notifica al Garante Privacy

Il disposto normativo GDPR, ai sensi dell'articolo 33, ha inoltre previsto fra gli ulteriori adempimenti in capo a tutte le organizzazioni che trattano dati personali, l'obbligo di notifica dell'avvenuta violazione dei dati personali al Garante per la Protezione dei Dati Personali. La notifica deve avere i seguenti requisiti:

- descrivere la natura della violazione dei Dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione;
- comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;

- descrivere le probabili conseguenze della violazione dei Dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione dei Dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica deve essere effettuata ove possibile entro 72 ore e senza "ingiustificato ritardo", da quando il Titolare è venuto a conoscenza del *Data Breach*.

2. Notifica agli Interessati

Nel caso in cui la violazione dei Dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli Interessati, il GDPR, ai sensi dell'art. 34, obbliga il Titolare del Trattamento a comunicare tale violazione anche a ciascun Interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi Dati personali.
La comunicazione del *Data Breach* all'Interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve contenere un'accurata descrizione della natura della violazione dei Dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei suoi Dati personali. Tuttavia, si può essere esonerati dalla notifica all'Interessato, ove:

- il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati personali oggetto della violazione;
- il Titolare del Trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- detta comunicazione richiederebbe sforzi sproporzionati, in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia;
- i contenuti delle comunicazioni violate sono interamente cifrati.

Art. 50 - Registro dei Data Breach

Ai sensi dell'art. 33 del GDPR è obbligatorio per il Titolare del Trattamento conservare la documentazione attestante tutti i *Data Breach* avvenuti. I Titolari sono, quindi, tenuti a conservare un registro dei *Data Breach* che deve essere tempestivamente aggiornato e contenere le seguenti informazioni:

- i dettagli relativi al *Data Breach* (e cioè la causa, il luogo dove è avvenuto e la tipologia di Dati personali violati);
- gli effetti e le conseguenze della violazione e il piano di intervento predisposto dal Titolare.

Oltre a questi aspetti, il Titolare dovrebbe anche motivare la ragione delle decisioni assunte a seguito del *Data Breach* con particolare riferimento ai seguenti casi:

- il Titolare ha deciso di non procedere alla notifica;
- il Titolare ha ritardato nella procedura di notifica;
- il Titolare ha deciso di non notificare il *Data Breach* agli Interessati.

ALLEGATO A - INTEROPERABILITÀ E FEDERAZIONE FRA I SISTEMI DI AUTENTICAZIONE

Infrastrutture di Autenticazione

L'infrastruttura di autenticazione di ateneo esegue la validazione dell'identità digitale della persona che richiede l'accesso alle risorse di un computer oppure di un sistema informativo.

I servizi di *directory* e di autenticazione sono stati consolidati su una piattaforma basata su *Microsoft Active Directory*. L'interoperabilità con apparati di rete, sistemi e applicativi eterogenei viene garantita da una serie di processi satellite che implementano protocolli quali *RADIUS*, *LDAPS*, *Kerberos* e *SAML*.

L'infrastruttura di autenticazione è utilizzata in modo trasparente dai singoli utenti ogni volta che tentano di accedere a un sistema informativo di ateneo digitando i propri nome utente e *password*.

Ai Dipartimenti e alle strutture regolarmente autorizzate viene concessa la possibilità di utilizzare l'infrastruttura di autenticazione di ateneo per controllare gli accessi ai propri sistemi informativi e postazioni informatiche mediante l'utilizzo di diversi protocolli.

Nei paragrafi seguenti sono riportate le modalità operative per l'interoperabilità di sistemi e applicativi eterogenei con l'infrastruttura di autenticazione di ateneo.

Kerberos e relazioni di fiducia tra domini basati su *Microsoft Windows*

Le strutture che gestiscono le proprie risorse informatiche (postazioni di lavoro, stampanti di rete, *file* e cartelle) mediante un servizio di *directory* basato su *Microsoft Active Directory - Directory Services* (livello funzionale Windows 2008) possono richiedere l'autorizzazione per l'impostazione di una relazione di fiducia in ingresso verso l'infrastruttura di autenticazione di ateneo.

Questo servizio risulta particolarmente utile nei seguenti scenari:

- Postazioni di lavoro per personale universitario (sia docente che tecnico amministrativo);
- Terminali ad accesso pubblico per personale universitario (sia docente che tecnico amministrativo) e studenti;
- Laboratori informatizzati.

Attraverso la relazione di fiducia, gli utenti gestiti mediante l'infrastruttura di autenticazione di ateneo potranno utilizzare le risorse informatiche messe a disposizione dal Dipartimento. In questo modo il Dipartimento non dovrà preoccuparsi di gestire le credenziali dei propri utenti.

Per attivare il servizio le fasi sono, sinteticamente, le seguenti:

N.	**Fase**	**Attore**
1	Pianificazione architettura	Struttura richiedente
2	Richiesta all'Area Sistemi Informativi attivazione servizio	Struttura richiedente
3	Attivazione eventuali IP *server*	Area Sistemi Informativi
4	Configurazione *server Domain ControllerDomain Controller*	Area Sistemi Informativi
5	Implementazione e configurazione *server Domain Controller*	Struttura richiedente
6	Test di autenticazione	Area Sistemi Informativi /Struttura richiedente

Gli aspetti di raggiungibilità IP tra *server* e *client*, potenzialmente distribuiti geograficamente e quindi attestati su sottoreti differenti o su sottoreti dotate di indirizzamento privato non ruotato, rappresentano il primo punto che deve essere definito e concordato. Il ruolo di *Domain Controller* dovrà essere eseguito su un calcolatore dotato di una interfaccia di rete con IP statico (preferibilmente privato ruotato). Le informazioni da fornire all'Area Sistemi Informativi durante la richiesta di attivazione del servizio sono quindi:

- Indirizzo IP Statico e nome *host* del *server*;
- Nome utente e *password* di un *account* avente privilegi amministrativi nel dominio della struttura richiedente.

Radius

Le strutture che gestiscono postazioni di lavoro informatizzate senza possedere un sistema di autenticazione centralizzato, possono richiedere l'autorizzazione per utilizzare l'infrastruttura di autenticazione di ateneo mediante il protocollo RADIUS o "*Remote Access Dial-In User Service*" per controllare l'accesso alle proprie postazioni di lavoro.

Questo servizio risulta particolarmente utile nei seguenti scenari:

- Postazioni di lavoro per personale universitario (sia docente che tecnico amministrativo);

- Terminali ad accesso pubblico per personale universitario (sia docente che tecnico amministrativo) e studenti;
- Laboratori informatizzati.

Il servizio basato sul protocollo RADIUS è inteso come puro servizio di autenticazione cioè come verifica della combinazione "nome utente" + "*password*".

A fronte di una richiesta di autenticazione, i *server* RADIUS dell'Area Sistemi Informativi forniranno una di due possibili risposte:

- "*access-accept*" in caso di combinazione corretta;
- "*access-reje*ct" in caso di combinazione errata.

I reami di autenticazione vengono interrogati senza possibilità di specificare alcuna struttura organizzativa o filtri su altri attributi localmente disponibili.

Il servizio prevede che la struttura richiedente configuri un *server* che operi da *proxy* RADIUS. Questo *server* verrà utilizzato direttamente e in piena autonomia dalla struttura per autenticare i propri *computer client* e si interfaccerà con i sistemi RADIUS gestiti dall' Area Sistemi Informativi in configurazione ridondata e geograficamente distribuita.

Oltre alla funzione di interfacciamento tra i sistemi dell'Area Sistemi Informativi e i *client*, il *server proxy* RADIUS gestito dalla struttura dovrà gestire i registri (*log*) delle richieste di autenticazione completi di indicazione della risposta di accettazione o rifiuto da parte dei *server* dell'Area Sistemi Informativi, ora e utente richiedente.

Per attivare il servizio le fasi sono, sinteticamente, le seguenti:

N.	Fase	Attore
1	Pianificazione architettura	Struttura richiedente
2	Richiesta all'Area Sistemi Informativi attivazione servizio	Struttura richiedente
3	Attivazione eventuali IP *server*	Area Sistemi Informativi
4	Configurazione *server* dell'Area Sistemi Informativi	Area Sistemi Informativi
5	Implementazione e configurazione *server* proxy Radius	Struttura richiedente
6	Test di connessione	Area Sistemi Informativi /Struttura richiedente
7	Configurazione client RADIUS	Struttura richiedente

LDAPS

Le strutture che gestiscono sistemi informativi senza possedere un sistema di autenticazione centralizzato, possono richiedere l'autorizzazione per utilizzare l'infrastruttura di autenticazione di ateneo mediante il protocollo *LDAPS* per controllare l'accesso ai propri sistemi informativi e applicazioni.

Questo servizio risulta particolarmente utile nei seguenti scenari:

- Postazioni di lavoro per personale universitario (sia docente che tecnico amministrativo);
- Terminali ad accesso pubblico per personale universitario (sia docente che tecnico amministrativo) e studenti;
- Laboratori informatizzati;
- Applicativi *Web* per personale universitario (sia docente che tecnico amministrativo) e studenti.

Il servizio prevede che la struttura richiedente configuri le postazioni di lavoro o *server* ospitante l'applicazione Web per utilizzare LDAPS quale protocollo di autenticazione. Le postazioni di lavoro o il *server* saranno configurati e utilizzati direttamente e in piena autonomia dalla struttura per autenticare gli utenti e si interfacceranno con l'infrastruttura di autenticazione di ateneo gestita dell'Area Sistemi Informativi in configurazione ridondata e geograficamente distribuita.

Oltre alla funzione di autenticazione verso i sistemi dell'Area Sistemi Informativi, il *server Web* gestito dalla struttura dovrà gestire i registri (*log*) delle richieste di autenticazione completi di indicazione della risposta di accettazione o rifiuto da parte dei *server* dell'Area Sistemi Informativi, ora e utente richiedente.

Per attivare il servizio le fasi sono, sinteticamente, le seguenti:

N.	**Fase**	**Attore**
1	Pianificazione architettura	Struttura richiedente
2	Richiesta all'Area Sistemi Informativi attivazione servizio	Struttura richiedente
3	Attivazione eventuali IP *server*	Area Sistemi Informativi
4	Configurazione *server* dell'Area Sistemi Informativi	Area Sistemi Informativi
5	Implementazione e configurazione *server*/applicativo della Struttura richiedente	Struttura richiedente
6	Test di connessione	Area Sistemi Informativi /Struttura richiedente
7	Configurazione client/applicativi della Struttura richiedente	Struttura richiedente

SAML

Attualmente i sistemi di autenticazione basati su protocolli *SAML* non offrono servizi a terzi, ma sono esclusivamente finalizzati ad alcune *suite* di prodotti:

- *Identity provider Shibboleth* presso Cineca: utilizzato per l'autenticazione su applicativi Cineca (*suite U-gov*, *Titulus*, *elearning*, etc.);
- *Active Directory Federation Service* (ADFS): utilizzato per l'autenticazione sulla *suite Microsoft Office 365*.

ALLEGATO B – SPECIFICHE TECNICHE E STANDARD PER LA RETE DATI DI ATENEO

Al fine di assicurare il buon funzionamento e la gestione della Rete dati di Ateneo - RDA, tutti gli *host* ad essa connessa devono attenersi alle presenti specifiche tecniche.
In caso di violazioni delle presenti norme, gli *host* potranno essere sconnessi dalla rete fino al loro adeguamento, o il loro accesso potrà venir limitato.
L'Area Sistemi Informativi non fornisce un servizio di filtraggio individuale per i singoli *host*.

- L'*host* deve rispettare le seguenti RFC generiche:
  a. RFC1122 - *Requirements for Internet Hosts -- Communication Layers* (ftp://ftp.rfc-editor.org/in-notes/rfc1122.txt) e successive modifiche e integrazioni;
  b. RFC1123 - *Requirements for Internet Hosts -- Application and Support* (ftp://ftp.rfc-editor.org/in-notes/rfc1123.txt) e successive modifiche e integrazioni;
  c. La scheda di rete utilizzata deve essere conforme alle specifiche IEEE802.3.
  d. L'*host* deve utilizzare esclusivamente il *mac address* assegnato dal produttore della scheda di rete per le schede fisiche, ed assegnato dall'ambiente di virtualizzazione per le schede delle macchine virtuali.
- L'*host* deve utilizzare esclusivamente l'indirizzo IP assegnato dall'Area Sistemi Informativi, mediante *DHCP* o assegnazione statica in seguito a richiesta sul portale *web* dell'Area Sistemi Informativi *On Line*. È vietato rispondere alle richieste ARP per indirizzi IP diversi da quello assegnato, e generare pacchetti IP con indirizzi IP sorgente diversi da quello assegnato.
- L'assegnazione di indirizzi IP dinamici tramite *DHCP* è valida esclusivamente per il tempo di *lease* fornito dal protocollo. È vietato configurare manualmente un indirizzo IP ottenuto tramite *DHCP*.
- L'assegnazione di indirizzi IP statici a seguito di richiesta sui SOL è valida fino a nuova comunicazione in merito da parte dell'Area Sistemi Informativi. Si fa presente che in casi eccezionali potrebbe essere necessario modificare l'indirizzo IP statico assegnato aun *host*, preservando comunque la validità del nome DNS.
- Per gli *host* che svolgono la funzione di *server*, è caldamente raccomandato l'utilizzo del nome DNS dell'*host*, e non quello del suo indirizzo IP, per la configurazione dei *client* relativi o/e per la comunicazione al pubblico, in quanto non è possibile garantire senza eccezioni il mantenimento dell'indirizzo IP assegnato.
- L'*host* deve usare un *client* DHCP conforme alla RFC2131 - *Dynamic Host Configuration Protocol* (ftp://ftp.rfc-editor.org/in-notes/rfc2131.txt) e successive modifiche e integrazioni.
- Eventuali *firewall software* installati sull'*host* devono accettare pacchetti UDP con porta sorgente 67 (*dhcp-server*) e porta destinazione 68 (*dhcp-client*).
- Ciascun *host* può farsi assegnare dal *server DHCP* un solo indirizzo IP per volta.

- L'*host* non deve agire come *server* DHCP, salvo nel caso di sottoreti private, e previa comunicazione preventiva all'Area Sistemi Informativi attraverso l'apposito modulo.
- L'*host* connesso alla rete deve avere sempre assegnato un indirizzo IP.
- Per consentire la verifica dell'utilizzo degli indirizzi IP, l'*host* deve rispondere al *ping* (*ICMP echo request/echo reply*) dalla rete di amministrazione dell'Area Sistemi Informativi (193.206.179.0/24) e dalla sottorete locale.

ALLEGATO C – NORMATIVA DI RIFERIMENTO

Direttiva dell'Unione Europea (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*

Regolamento dell'Unione Europea (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*

Decreto Legislativo 10 agosto 2018, n. 101, *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*

Decreto Legislativo 13 dicembre 2017, n. 217, *Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.*

Decreto Legislativo 26 agosto 2016, n. 179, *Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*

Decreto Legislativo 7 marzo 2005, n. 82 e ss.mm.ii, *Codice dell'amministrazione digitale.*

Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i *Codice in materia di protezione dei dati personali* come modificato dal Decreto legislativo 101/18.

Agenzia per l'Italia Digitale – AgID, Circolare 18 aprile 2017, n. 2/2017 *Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015).*

Istruzioni, linee guida e documentazione informativa

Linee guida dell'Agenzia per l'Italia Digitale – AgID 26 aprile 2016, *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015).*

European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016*.

European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on the right to data portability Adopted on 13 December 2016*.

Garante per la protezione dei dati personali, Provvedimento del 13 luglio 2016, n. 303 relativo al trattamento dei dati personali dei dipendenti mediante la posta elettronica ed altri strumenti di lavoro;

Garante per la protezione dei dati personali, Provvedimento del 3 ottobre 2013, n. 429 *Prescrizioni per il trattamento di dati di traffico telefonico e telematico.*

Garante per la protezione dei dati personali, Provvedimento del 25 giugno 2009 *Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento*

Garante per la protezione dei dati personali, Provvedimento del 27 novembre 2008, *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.*

Garante per la protezione dei dati personali, Provvedimento del 17 gennaio 2008, *Sicurezza dei dati di traffico telefonico e telematico*

Garante per la protezione dei dati personali, Deliberazione del 1° marzo 2007, n. 13 *Lavoro: le linee guida del Garante per posta elettronica e internet*

ALLEGATO D – MISURE MINIME DI SICUREZZA PER ABSC 5.7.1, 5.7.3, 8.1.1, 8.1.2, 8.7.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1 e 13.1.1

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica

ALLEGATO E – DOCUMENTO RELATIVO ALLE MISURE MINIME DI SICUREZZA PER LE STRUTTURE

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID	Livello	Descrizione	Modalità di implementazione

2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	

4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	

5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	

5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	

8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	
8	9	2	M	Filtrare il contenuto del traffico web.	
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	

10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio	

				attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

ALLEGATO F – PROCEDURA PER LA GESTIONE DEI *DATA BREACH*

DEFINIZIONI COMUNI

Nel proseguo del presente documento sono adottate le seguenti definizioni:

1. **Struttura d'Ateneo**: ogni entità autonoma facente parte dell'Ateneo (Dipartimenti, Scuola di Medicina, Centri di Ricerca, Centri Speciali, Aree dell'Amministrazione Centrale, etc.).
2. **Responsabile di struttura**: Direttore Generale, Dirigente di Area dell'Amministrazione Centrale, Direttore di Dipartimento, Direttore di centro speciale, Presidente Scuola di Medicina.
3. **ASI**: Area Sistemi Informativi.
4. **Responsabile per la transizione digitale**: nominato dall'Ateneo ai sensi dell'art. 17 del D. Lgs 5 marzo 2005, n. 82 e ss.mm.ii (Codice Amministrazione Digitale).
5. **Referente Privacy**: Dirigente incaricato quale referente privacy dell'Ateneo.
6. **GDPR:** Regolamento dell'Unione Europea (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*.
7. **WP29**: Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art.29 della Direttiva Europea 95/46.
8. **DPO**: Responsabile della Protezione dei dati Personali ai sensi dell'art. 37 del Regolamento dell'Unione Europea (UE) 2016/6.
9. **Consenso**: manifestazione di volontà libera, specifica e informata dell'interessato con cui questi accetta espressamente che i suoi dati personali siano fatti oggetto di trattamento.
10. **Dati Biometrici**: dati ricavati da proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità.
11. **Dati Genetici**: dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisiche che forniscono informazioni uniche sulla fisiologia o sulla salute della stessa, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
12. **Dati Giudiziari**: dati che rilevano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. provvedimenti penali di condanna definitivi, liberazione condizionale, divieto od obbligo di soggiorno, misure alternative alla detenzione).
13. **Dati personali**: qualunque informazione relativa ad una persona fisica, identificata od identificabile, anche indirettamente, attraverso altre informazioni, ivi compreso un numero di identificazione personale.
14. **Dati sanitari**: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative allo stato di salute.
15. **Dati sensibili**: dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati o associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i Dati personali idonei a rilevare lo stato di salute e la vita sessuale.

16. **Destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
17. **Garante**: Autorità garante per la protezione dei Dati personali, vale a dire l'Autorità nazionale di controllo ("Anc") preposta alla vigilanza ed al controllo della normativa sulla protezione dei Dati personali.
18. **Finalità**: scopo determinato, esplicito e legittimo che viene perseguito dal Titolare del trattamento.
19. **Incaricato del trattamento (soggetto autorizzato)**: persona fisica autorizzata a compiere operazioni di trattamento sulla base delle istruzioni ricevute dal Titolare o dal Responsabile.
20. **Informativa**: documento contenente le informazioni che il Titolare deve fornire all'Interessato per chiarire se quest'ultimo è obbligato o meno a rilasciare i dati personali, le conseguenze di un eventuale rifiuto al rilascio degli stessi, quali sono le finalità e le modalità del trattamento, i soggetti che entrano in contatto con i suoi dati personali, come circolano i dati personali ed in che modo esercitare i diritti riconosciuti dal GDPR.
21. **Interessato**: persona fisica cui si riferiscono i Dati personali.
22. **Responsabile (del Trattamento)**: persona, fisica o giuridica, Pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al Trattamento.
23. **Titolare (del Trattamento)**: persona, fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro Titolare, le decisioni in ordine alle Finalità, alle modalità del Trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
24. **Trattamento**: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la
comunicazione, la diffusione, la cancellazione e la distruzione di dati personali, anche se non registrati in una banca dati.

IL *DATA BREACH* E GLI ADEMPIMENTI CORRELATI

L'articolo 4 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, sancisce che una violazione dei dati personali ("*Data Breach*") è "una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Il Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art.29 della Direttiva Europea 95/46, con le linee guida WP250, ha meglio precisato che i *Data Breach* sono classificabili in tre macro-categorie:

1. "*Confidentiality Breach*", quando vi è un accesso accidentale o abusivo a Dati personali;
2. "*Availability Breach*", quando vi è una perdita o distruzione accidentale o non autorizzata del Dato personale;
3. "*Integrity Breach*", quando vi è un'alterazione accidentale o non autorizzata del Dato personale

Notifica al Garante per la Protezione dei Dati Personali (ex art. 33 del GDPR)

Il disposto normativo GDPR, ai sensi dell'articolo 33, ha inoltre previsto fra gli ulteriori adempimenti in capo a tutte le organizzazioni che trattano dati personali, l'obbligo di notifica dell'avvenuta violazione dei dati personali al Garante per la Protezione dei Dati Personali; la notifica deve avere i seguenti requisiti:

- descrivere la natura della violazione dei Dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione;
- comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei Dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione dei Dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica deve essere effettuata ove possibile entro 72 ore e senza "ingiustificato ritardo", da quando il Titolare è venuto a conoscenza del *Data Breach*.

Notifica agli Interessati (ex art.34 del GDPR)

Nel caso in cui la violazione dei Dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli Interessati, il GDPR obbliga il Titolare del Trattamento a comunicare tale violazione anche a ciascun Interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi Dati personali.
La comunicazione del *Data Breach* all'Interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve contenere un'accurata descrizione della natura della violazione dei Dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti

negativi derivanti dalla violazione dei suoi Dati personali. Tuttavia, si può essere esonerati dalla notifica all'Interessato, ove:

- il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati personali oggetto della violazione;
- il Titolare del Trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
- detta comunicazione richiederebbe sforzi sproporzionati, in tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia;
- i contenuti delle comunicazioni violate sono interamente cifrati.

Registro dei *Data Breach*

Ai sensi dell'art. 33 del GDPR è obbligatorio per il Titolare del Trattamento conservare la documentazione attestante tutti i *Data Breach* avvenuti. I Titolari sono, quindi, tenuti a conservare un registro dei *Data Breach* che deve essere tempestivamente aggiornato e contenere le seguenti informazioni:

- i dettagli relativi al *Data Breach* (e cioè la causa, il luogo dove è avvenuto e la tipologia di Dati personali violati);
- gli effetti e le conseguenze della violazione e il piano di intervento predisposto dal Titolare.

Oltre a questi aspetti, il Titolare dovrebbe anche motivare la ragione delle decisioni assunte a seguito del *Data Breach* con particolare riferimento ai seguenti casi:

- il Titolare ha deciso di non procedere alla notifica;
- il Titolare ha ritardato nella procedura di notifica;
- il Titolare ha deciso di non notificare il *Data Breach* agli Interessati.

Tipologie di Data Breach

Gli eventi che possono causare un *Data Breach* sono così raggruppati nell'articolo 4(12) del GDPR sulla base delle linee guida ENISA:

- *Unauthorized Access*: accesso ai dati da parte di soggetti (interni o esterni) non aventi diritto;
- *Loss*: indisponibilità temporanea dei dati;
- *Destructio*n: indisponibilità irreversibile dei dati;
- *Transmission*: comunicazione (fortuita o intenzionale) dei dati verso destinatari non autorizzati;
- *Alteration or Modification*: modifica impropria (accidentale o intenzionale) dei dati;
- *Disclosure*: divulgazione impropria di informazioni riservate.

L'INCIDENT RESPONSE TEAM DEL DATA BREACH

Nel seguito si descrivono composizione, competenze ed adempimenti in carico alle risorse organizzative che Università degli Studi dell'Insubria ha deciso di approntare per le attività connesse alla identificazione, gestione e comunicazione dei *Data Breach* ai sensi del GDPR.
Il team ha il compito di

- eseguire l'analisi dell'evento al fine di valutare se si tratti di un *Data Breach;*
- provvedere se necessario a effettuare la procedura di notifica *data breach*,
- predisporre se necessario la notifica agli *interessati.*

L'Incident Response Team del Data Breach riporta direttamente al Direttore Generale ed al Titolare dei Dati (Magnifico Rettore).

Tenendo conto delle finalità, tipologia di utenza e assetto organizzativo dell'Ateneo, sono stati individuati tre ambiti operativi omogenei secondo cui classificare l'afferenza di un *Data Breach*, in analogia a quanto implementato relativamente all'applicazione delle Misure minime di sicurezza informatica per le Pubbliche Amministrazioni ai sensi della Circolare 18 aprile 2017, n. 2 dell'Agenzia per l'Italia Digitale – AgID:

- **Ambito Gestione ed Amministrazione**: a questo ambito appartengono i dati con principali finalità di gestione ed amministrazione dell'Ateneo.
- **Ambito Ricerca**: a questo ambito appartengono i dati con principali finalità di ricerca.
- **Ambito Didattica**: a questo ambito appartengono i dati finalizzati all'erogazione dell'attività didattica dell'Ateneo.

Nei singoli tre ambiti Gestione/Ricerca e Didattica, i Data Breach sono ulteriormente classificabili in eventi che coinvolgono sistemi informatizzati ed eventi senza coinvolgimento di sistemi informatizzati.

La composizione dell'Incident Response Team Data Breach è declinata a seconda degli specifici ambiti come di seguito dettagliato.

L'Incident Response Team Data Breach, in caso di necessità, si può avvalere della collaborazione dei responsabili delle Unità Organizzative coinvolte nell'incidente o il cui coinvolgimento è utile all'analisi, identificazione e gestione dell'incidente stesso.

Composizione Incident Responce Team Data Breach

L'Incident Responce Team Data Breach è composto da membri con profili differenziati di tipo manageriale, legale e tecnico; il team ha lo scopo di gestire i *Data Breach* dal punto di vista organizzativo, legale e tecnico, nonché identificare, gestire e comunicare in modo efficace e tempestivo ogni eventuale incidente che possa configurare un *Data Breach.*

L'Incident Response Team Data Breach si può avvalere della collaborazione di ulteriori elementi, tipicamente di professionisti ICT per l'analisi ed il contrasto dei data beach in ambito ICT e dei Responsabili del Trattamento, questi ultimi anche in ottemperanza al principio di responsabilità solidale fra il Titolare dei Dati ed i Responsabili del Trattamento, definita nell'articolo 82 del GDPR.

Al fine di perseguire la massima efficacia e competenza dell'*Incident Response Team Data Breach*, a seconda dell'ambito omogeneo a cui è ascrivibile un potenziale *Data Breach*, i membri effettivi dell'*Incident Response Team Data Breach* sono così individuati:

TABELLA 1 – TEAM PER DATA BREACH

Profilo Professionale	Ambito Gestione ed Amministrazione	Ambito Ricerca	Ambito Didattica
Competenze Legali ambito Privacy	Data Protection Officer	Data Protection Officer	Data Protection Officer
Competenze Manageriali con funzione di Coordinatore del Team	Referente Privacy di Ateneo	Referente Privacy di Ateneo	Referente Privacy di Ateneo
Competenze specifiche di ambito del trattamento	Responsabili delle strutture a cui fanno capo i trattamenti interessati (come dichiarato nel registro dei trattamenti) o loro delegati	Responsabili delle strutture a cui fanno capo i trattamenti interessati (come dichiarato nel registro dei trattamenti) o loro delegati	Responsabili delle strutture a cui fanno capo i trattamenti interessati (come dichiarato nel registro dei trattamenti) o loro delegati
Supporto amministrativo	Ufficio Organizzazione, trasparenza e prevenzione della corruzione	Ufficio Organizzazione, trasparenza e prevenzione della corruzione	Ufficio Organizzazione, trasparenza e prevenzione della corruzione
Competenze Tecniche ICT (solo per Data Breach che coinvolgono trattamenti con sistemi informatici)	Composizione come da Tabella 2	Composizione come da Tabella 2	Composizione come da Tabella 2

Le competenze ICT organiche all'IRT sono declinate in numerosità e tipologia a secondo della specificità del Data Beach o potenziale Data Breach in esame, come di seguito dettagliato.

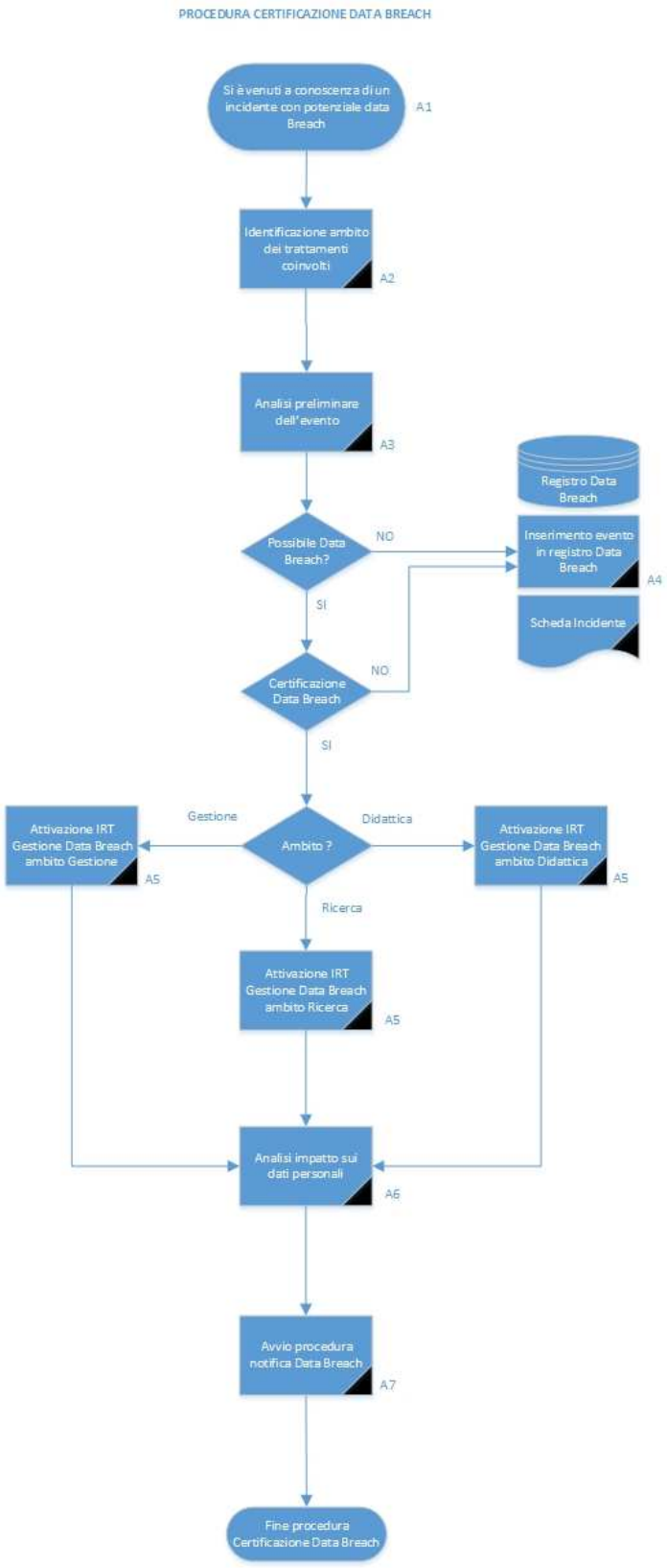
TABELLA 2

Profilo Professionale	Sistemi informatici o Asset esclusivamente afferenti ad ASI	Sistemi informatici o Asset esclusivamente afferenti ad un Dipartimento	Sistemi informatici o Asset afferenti che coinvolgano sia ASI che un Dipartimento
Competenze Tecniche ICT	Responsabile Servizio S-DIG Responsabie Servizio S-FOF	Tecnico informatico dipartimentale	Tecnico informatico dipartimentale Responsabile Servizio S-DIG Responsabie Servizio S-FOF

PROCEDURA CERTIFICAZIONE *DATA BREACH*

La procedura di Certificazione di una *Data Breach* viene avviata ogni qualvolta il Titolare dei Dati, un CoTitolare dei dati, un Responsabile di Struttura, un Autorizzato al trattamento, un Interessato, indentifichi o venga informato di una violazione di sicurezza che possa comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (*Data Breach*). La procedura deve essere avviata senza indugio e conclusa nel più breve tempo possibile. Ogni qualvolta la procedura viene avviata, deve essere effettuata apposita registrazione dell'evento nel registro dei *Data Breach* di Università degli Studi dell'Insubria.

La segnalazione di un incidente con potenziale *Data Breach*, viene effettuata scrivendo alla casella email privacy@uninsubria.it, la segnalazione può essere effettuata sia da personale appartenente all'Organizzazione sia da persone esterne ad essa.


PROCEDURA CERTIFICAZIONE DATA BREACH
Si è venuti a conoscenza di un incidente con potenziale data Breach
A1
Identificazione ambito dei trattamenti coinvolti
A2
Analisi preliminare dell'evento
A3
Registro Data Breach
Possibile Data Breach?
NO
Inserimento evento in registro Data Breach
A4
Scheda Incidente
SI
Certificazione Data Breach
NO
SI
Gestione
Ambito ?
Didattica
Attivazione IRT Gestione Data Breach ambito Gestione
A5
Attivazione IRT Gestione Data Breach ambito Didattica
A5
Ricerca
Attivazione IRT Gestione Data Breach ambito Ricerca
A5
Analisi impatto sui dati personali
A6
Avvio procedura notifica Data Breach
A7
Fine procedura Certificazione Data Breach

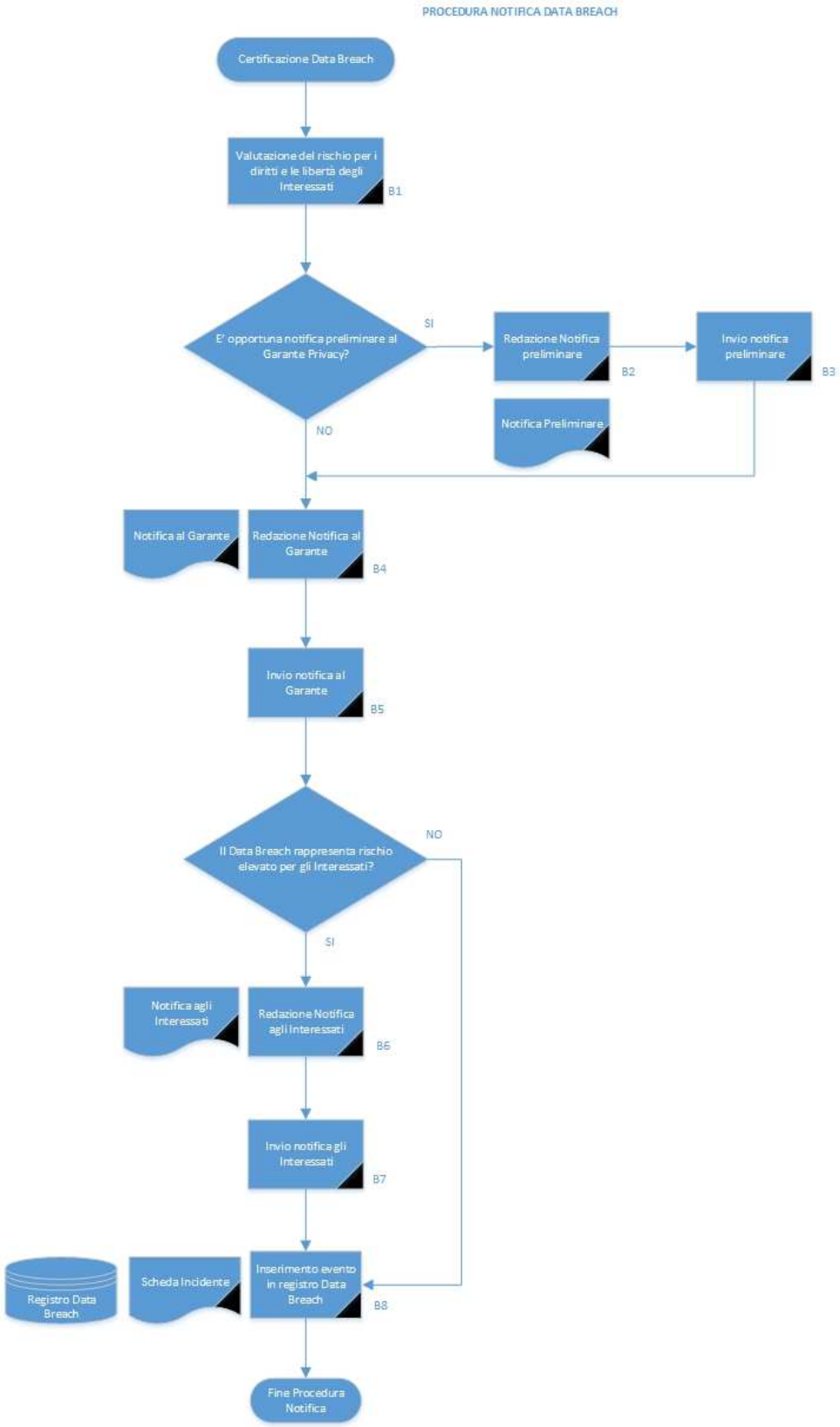
Matrice RACI della procedura Certificazione *Data Breach*:

ID	Nome Attività	Descrizione	RACI				Tempo di esecuzione	
			R	A	C	I	Avvio	Termine
A1	Ricevimento segnalazione potenziale data Breach	Ricezione di una segnalazione di potenziale Data Breach all'indirizzo privacy@uninsubria.it	RP	ORGANIZZA				
A2	Identificazione ambito di appartenenza e trattamenti coinvolti	Identificare l'ambito a cui si riferisce la segnalazione, se riguarda trattamento con strumenti informatici oppure no, identificare voci del registro trattamenti coinvolte	RP	ORGANIZZA				
A3	Analisi Preliminare evento	Analizzare in via preliminare l'incidente occorso al fine di verificare il potenziale accadimento di un *Data Breach*	RP	RT	ORGANIZZA		appena venuti a conoscenza dell'incidente	il prima possibile
A4	Registrazione Incidente	Registrare l'incidente nel registro dei *Data Breach*	RP	ORGANIZZA		DPO	il prima possibile	il prima possibile
A5	Attivazione IRT	Notificare potenziale *Data Breach* al IRT	RP	ORGANIZZA		DPO	il prima possibile	il prima possibile
A6	Analisi Impatto su dati Personali	Analizzare l'incidente certificando l'eventuale *Data Breach* occorso o in atto	DPO	IRT	RT		il prima possibile	il prima possibile
A7	Avvio procedura notifica *Data Breach*	Avviare la procedura di gestione dei *Data Breach*	RP	ORGANIZZA		DPO	il prima possibile	il prima possibile

Legenda Simboli			
ID	Identificativo attività con riferimento al diagramma di flusso	**DPO**	Data Protection Officer
R	Responsabile: coordina l'attività	**T**	Titolare dei dati (Magnifico Rettore)
A	Si occupa di eseguire l'attività	**RT**	Responsabile di struttura
C	Collabora all'esecuzione dell'attività	**CT**	CoTitolare del Trattamento dei dati
I	E' informato su andamento ed esito attività	**RP**	Referente Privacy
IRT	Incident Response Team Data Breach	**ORGANIZZA**	Ufficio Organizzazione, trasparenza e prevenzione della corruzione

Procedura Notifica *Data Breach*

A valle della certificazione dell'evento di sicurezza come *Data Breach,* deve essere avviata senza indugio la seguente procedura della notifica del *Data Breach* nei tempi indicati dalla normativa (72 ore dall'avvenuta conoscenza del *Breach*) prevedendo se necessario alla *Notifica* da inviare al Garante Privacy secondo il modello pubblicato sul sito web dell'Autorità.


PROCEDURA NOTIFICA DATA BREACH
Certificazione Data Breach
Valutazione del rischio per i diritti e le libertà degli Interessati
B1
E' opportuna notifica preliminare al Garante Privacy?
SI
Redazione Notifica preliminare
B2
Invio notifica preliminare
B3
Notifica Preliminare
NO
Notifica al Garante
Redazione Notifica al Garante
B4
Invio notifica al Garante
B5
Il Data Breach rappresenta rischio elevato per gli Interessati?
NO
SI
Notifica agli Interessati
Redazione Notifica agli Interessati
B6
Invio notifica gli Interessati
B7
Registro Data Breach
Scheda Incidente
Inserimento evento in registro Data Breach
B8
Fine Procedura Notifica

Matrice RACI della Notifica *Data Breach*:

ID	Nome Attività	Descrizione	RACI				Tempo di esecuzione	
			R	A	C	I	Avvio	Termine
B1	Valutazione Rischi	Valutare se il *Data Breach* può rappresentare dei rischi per i diritti e le libertà degli Interessati	DPO	IRT	RP		immediato	il prima possibile
B2	Redazione Notifica Preliminare	redazione della notifica preliminare di *Data Breach* per il Garante Privacy	T	DPO	IRT		il prima possibile	il prima possibile
B3	Invio Notifica Preliminare *Data Breach*	Invio al Garante Privacy della notifica preliminare di *Data Breach*	DPO	ORGANIZZA	IRT	T;CT	il prima possibile	entro 72 ore da avvio processo
B4	Redazione notifica Data Breach	Redazione della notifica di *Data Breach* per il Garante Privacy	T	DPO	IRT		il prima possibile	il prima possibile
B5	Invio Notifica *Data Breach*	Invio al Garante Privacy della notifica di *Data Breach*	DPO	ORGANIZZA		T;CT	il prima possibile	entro 72 ore da avvio processo
B6	Redazione notifica agli Interessati	Approntare una notifica agli Interessati fornendo anche indicazioni su come potersi proteggere dal Breach	T	DPO	IRT		il prima possibile	il prima possibile
B7	Invio Notifica agli Interessati	Invio agli interessati della notifica di *Data Breach* con indicazioni sul come proteggersi	DPO	ORGANIZZA		T;CT	il prima possibile	il prima possibile
B8	Registrazione *Data Breach*	Registrazione dell'evento di *Data Breach* nel *Registro dei Data Breach*	RP	ORGANIZZA		DPO	il prima possibile	il prima possibile

Legenda Simboli			
ID	Identificativo attività con riferimento al diagramma di flusso	**RP**	Referente Privacy
R	Responsabile: coordina l'attività	**DPO**	Data Protection Officer
A	Si occupa di eseguire l'attività	**T**	Titolare dei dati (Magnifico Rettore)
C	Collabora all'esecuzione dell'attività	**RT**	Responsabile di struttura
I	E' informato su andamento ed esito attività	**CT**	CoTitolare del Trattamento dei dati
IRT	Incident Response Team Data Breach	**ORGANIZZA**	Ufficio Organizzazione, trasparenza e prevenzione della corruzione

All. A – Normativa di riferimento

- Regolamento dell'Unione Europea (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*
- Decreto Legislativo 26 agosto 2016, n. 179, *Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*
- Direttiva dell'Unione Europea (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.*
- Decreto Legislativo 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale.*
- Decreto Legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali.*

All. B – Istruzioni, linee guida e documentazione

- WP 250 rev.01 – *Guidelines on Personal Data Breach Notification Under Regulation 2016/679* (Documento del Working Party Art. 29 adottato il 6 febbraio 2018).
- WP251 rev.01 – Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. (Documento del Working Party Art. 29 adottato il 3 ottobre 2017 e emendato il 6 febbraio 2018)
- WP248. Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017
- Linee guida dell'Agenzia per l'Italia Digitale – AgID 26 aprile 2016, *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni – Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015).*
- European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016.*
- European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on the right to data portability Adopted on 13 December 2016.*

All. C – Classificazione ed esempi di *Data Breach*

II Gruppo di lavoro dei Garanti Europei, ai sensi dell'ex art.29 della Direttiva Europea 95/46, di seguito WP29, ha classificato i *Data Breach* in base a tre macro-categorie:

1. "*Confidentiality Breac*h", quando vi è un accesso accidentale o abusivo a Dati personali;
2. "*Availability Brea*ch", quando vi è una perdita o distruzione accidentale o non autorizzata del Dato personale;
3. "*Integrity Breach*", quando vi è un'alterazione accidentale o non autorizzata del Dato personale

Per meglio contestualizzare il riconoscimento dei *Data Breach* in Università degli Studi dell'Insubria, di seguito vengono proposti alcuni casi a titolo esemplificativo ma non esaustivo:

Tipologia *Data Breach*	Esempio	Necessita Notifica a Garante Privacy?	Necessita Notifica agli interessati?	Note
Confidentiality Breach	Furto o smarrimento di Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati non cifrati o cifrati con algoritmi non allo stato dell'arte	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Furto o smarrimento di Chiavetta USB o Notebook o Tablet o Smartphone o Hard Disk su cui sono memorizzati dati cifrati con algoritmi allo stato dell'arte	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Confidentiality Breach	Una applicazione informatica subisce un attacco informatico a fronte del quale gli attaccanti hanno avuto accesso a dati personali e c'è il ragionevole sospetto che li abbiano consultati e/o sottratti (esempi di applicativi: Gestione Documentale *Titulus*, Gestione carriera studenti *Esse3,* Gestione del personale *Ugov Risorse Umane*, Gestione Diritto allo	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	

Tipologia *Data Breach*	Esempio	Necessita Notifica a Garante Privacy?	Necessita Notifica agli interessati?	Note
	studio, Gestione prestito bibliotecario, Servizio di Posta Elettronica e collaboration *Microsoft 365*, etc.)			
Availability Breach	Temporanea non disponibilità di un server, un applicativo o della connettività di rete (ad esempio per mancanza energia elettrica, guasto degli apparati)	NO	NO	Non deve essere notificato, ma l'incidente va inserito nel registro dei Data Breach
Confidentiality Breach/ *Availability Breach*	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati, non esiste un BackUp dei dati e/o c'è una ragionevole evidenza che i dati personali possono essere stati esfiltrati dal dispositivo	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Availability Breach	Una postazione di lavoro, o un server vengono compromessi da un Ransomware e conseguentemente i dati vengono cifrati, esiste un BackUp dei dati per cui possono essere ripristinati in tempi ragionevoli e c'è una ragionevole evidenza che i dati personali non sono stati sottratti dal dispositivo	NO	NO	Non deve essere notificato, ma va inserito nel registro dei Data Breach
Confidentiality Breach	Un titolare di credenziali di accesso a sistemi informatici che trattano dati personali segnala una perdita di confidenzialità delle proprie credenziali (ad esempio per aver dato seguito ad un messaggio di Phishing), da una veloce investigazione risulta che le credenziali siano state usate per accedere a dati personali con attività non	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	

Tipologia *Data Breach*	Esempio	Necessita Notifica a Garante Privacy?	Necessita Notifica agli interessati?	Note
	riconducibili all'utente autorizzato			
Confidentiality Breach	A seguito di un attacco informatico sono state trafugate le credenziali di utenze con privilegi di accesso a dati personali, tali credenziali erano memorizzati sul server in modalità non cifrata o cifrate con algoritmi non allo stato dell'arte o con meccanismi di cifratura non reversibile (hash) non allo stato dell'arte.	SI	SI	
Confidentiality Breach	A seguito di un errore di programmazione e configurazione di un sistema informatico o di una applicazione informatica, sono stati resi accessibili dati personali a soggetti non Autorizzati al trattamento o diversi dagli Interessati,	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Comunicazione di dati personali ad errato destinatario (ad esempio per invio ad indirizzo email errato)	SI	SI se la natura dei dati e la gravità del furto può avere importanti conseguenze per gli interessati	
Confidentiality Breach	Invio a mailing list di uno o più messaggi con gli indirizzi email dei destinatari in chiaro nel campo 'A' o nel campo 'CC'	SI se l'evento coinvolge un largo numero di individui	Dipende dallo scopo e dalla finalità della mailing list	