UNIVERSITÀ DEL PIEMONTE ORIENTALE

Regolamento di Ateneo per la sicurezza informatica

Sommario

Premessa

L'Università degli Studi del Piemonte Orientale (d'ora in poi definita Ateneo) ritiene indispensabile l'adozione di tecnologie informatiche e telematiche per lo svolgimento delle proprie attività istituzionali e per il miglioramento costante dei servizi offerti all'utenza, e ritiene altresì che l'utilizzo della rete Internet sia un imprescindibile strumento per garantire la più ampia visibilità e diffusione delle informazioni relative alla propria attività istituzionale.

L'Ateneo adotta adeguati controlli per tutelare la riservatezza, l'integrità e la disponibilità dei dati secondo le buone pratiche e gli standard in materia di sicurezza delle informazioni, in ottemperanza agli obblighi normativi esistenti (Leggi in materia di protezione dei dati personali *D. Lgs 196/2003* aggiornato al *D. Lgs 101/2018 - Codice in materia di protezione dei dati personali, Regolamento Europeo - Regolamento UE 2016/679* (di seguito "GDPR"), Provvedimenti dell'Autorità Garante per la protezione dei dati personali e linee guida del Comitato Europeo per la protezione dei dati personali (EDPB), *D.lgs. 7 marzo 82/2005* e successive modifiche - *Codice dell'Amministrazione digitale*, *Circolare 18 aprile 2017, n.2/2017*, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni» *Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015*).

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi a principi di responsabilità, diligenza e correttezza espressi all'interno del ***Codice Etico*** ed essere finalizzato esclusivamente ad attività previste nel quadro dell'attività istituzionale, amministrativa, di didattica di ricerca e di terza missione, l'Ateneo adotta una politica interna per l'attuazione e la diffusione di una cultura in materia di sicurezza informatica a tutela dell'**integrità**, della **disponibilità** e della **riservatezza delle informazioni**.

1. Obiettivi

Il presente Regolamento ha i seguenti obiettivi:

- **prevenire**, ove possibile, comportamenti anche inconsapevoli che possano minacciare o compromettere la sicurezza nel trattamento dei dati e/o l'accesso stesso alle risorse informatiche e telematiche dell'Ateneo;
- **codificare** le regole di comportamento da seguire per un corretto utilizzo degli strumenti e servizi onde evitare problemi, disservizi, costi aggiuntivi e rischi per la sicurezza dei dati, del patrimonio e della reputazione dell'Ateneo;
- **preservare** la sicurezza nell'accesso alla rete interna e alla rete Internet;
- **garantire** il rispetto delle leggi in materia di utilizzo delle risorse informatiche per l'elaborazione dei dati personali ai sensi delle Leggi in materia di protezione dei dati personali e normativa nazionale di settore;
- **informare** con chiarezza e trasparenza gli interessati sulle attività di monitoraggio e controllo;
- **diffondere** una cultura della sicurezza che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.

2. Ambito di applicazione

Il presente Regolamento si applica all'intero Ateneo, per tutte le sue sedi e riguarda tutti le risorse umane, fisiche e virtuali; è destinato agli individui e al personale a vario titolo coinvolto nelle attività dell'Ateneo ed a tutti coloro che utilizzano i servizi ICT dell'Ateneo, e definisce le politiche adottate a garanzia della sicurezza delle informazioni trattate direttamente dall'Ateneo alle quali devono uniformarsi anche i fornitori/outsourcer di servizi/attività funzionali all'erogazione dei servizi ICT.

A mero titolo esemplificativo e non esaustivo, i soggetti tenuti al rispetto del presente regolamento sono:

- Professori e ricercatori (Professori Ordinari, Professori Associati, Ricercatori, Professori emeriti, Professori onorari, Visiting Professor e Researcher);
- Personale Tecnico Amministrativo;
- Dottorandi;
- Borsisti di ricerca;
- Assegnisti di ricerca;
- Specializzandi;
- Studenti (studenti regolarmente iscritti in corsi di studio istituzionali. Tra i quali: studenti Erasmus, studenti iscritti a corsi interateneo);
- Collaboratori con cui intercorre un rapporto di lavoro formalizzato o di collaborazione a qualsiasi titolo a tempo determinato;
- Consulenti e fornitori;
- Spin-off e start-up;
- Società ed Enti esterni;
- Ospiti.

Nel caso di comportamenti o azioni caratterizzati dall'inosservanza del presente regolamento, da cui derivino danni per l'Ateneo o per i propri dipendenti, studenti, ecc, opereranno i profili di responsabilità civile, amministrativa, e penale previsti dalla normativa, nonché dallo Statuto e regolamenti dell'Ateneo.

3. Struttura organizzativa

Per un efficace presidio della sicurezza informatica è prevista una struttura organizzativa che integra le disposizioni previste per le pubbliche amministrazioni con lo specifico ordinamento dell'Università.

L'individuazione di linee strategiche inerenti la sicurezza Informatica, nonché l'adozione e revisione del presente regolamento, spettano al Consiglio di Amministrazione, su proposta del Rettore, sentito il Senato Accademico per gli aspetti di competenza. Per supportare gli sviluppi delle politiche della sicurezza sono individuati i seguenti attori / uffici, che cooperano attraverso prassi integrate,

caratterizzate da un approccio autonomo e responsabile, nell'ambito dell'architettura multicentrica dell'Ateneo.

Delegato del Rettore per la Transizione Digitale e/o Sicurezza Informatica – Figura di elevata qualificazione scientifico - disciplinare che può essere individuata dal Rettore per rafforzare l'integrazione tra le missioni istituzionali dell'Ateneo e lo sviluppo delle politiche per la sicurezza informatica.

Responsabile per la Transizione Digitale (RTD) – Figura che, ai sensi del Codice per l'Amministrazione Digitale (art. 17 D.lgs. 82/2005 e ss.mm.ii.), ha 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 del suddetto Codice.

Struttura deputata alla direzione dei sistemi informativi – Ha compiti direttivi connessi al presidio della sicurezza informatica secondo principi di efficienza, efficacia, economicità, nonché integrazione con le politiche per il trattamento dati e l'assicurazione della qualità previste dall'Ateneo; il relativo responsabile assume le funzioni di cui al punto precedente, laddove gli sia attribuito l'incarico di RTD.

Struttura deputata al coordinamento della sicurezza Informatica – Settore / Staff tipicamente dipendente dalla suddetta struttura dirigenziale, che assicura l'attuazione delle politiche di sicurezza previste dal presente regolamento ed il presidio evolutivo delle infrastrutture fisiche e logiche volte alla gestione della sicurezza, definendo le prassi gestionali ed operative che devono essere adottate dall'Ateneo, in coerenza con le linee strategiche per la sicurezza informatica e con il presente Regolamento. Ha la responsabilità della gestione in sicurezza degli asset assegnati, tipicamente a valenza di Ateneo.

Strutture ICT deputate alla gestione ed assistenza ICT delle sedi – Strutture deputate alla gestione dei servizi ICT decentrati (ad es. in logica di Polo), chiamate all'attuazione del Regolamento sulla base degli indirizzi e delle prassi definite dalle strutture sopra richiamate. Ha la responsabilità della gestione in sicurezza degli asset assegnati, tipicamente in relazione alla sede territoriale di competenza.

Direttrice / Direttore di Dipartimento o altro Centro autonomo di gestione – Figura che, nell'ambito della funzione della Direzione delle attività di didattica, ricerca e terza missione della propria struttura, autorizza l'attuazione di specifiche procedure di sicurezza che siano funzionalmente necessarie nell'ambito delle attività di ricerca e sviluppo, anche in deroga alle disposizioni generali, ove previsto dalle disposizioni normative, sentita la struttura dirigenziale competente per la sicurezza informatica.

Responsabile scientifico assegnatario di strumentazione informatica finalizzata ad attività di ricerca e sviluppo – Assume la responsabilità di gestire in sicurezza l'asset assegnato, con l'obiettivo di massimizzarne il livello di sicurezza fisica e logica, rispetto agli standard previsti, in relazione agli obiettivi dell'attività di ricerca e sviluppo da condurre. A tale fine sottoscrive idoneo documento che esplicita le relative policy di sicurezza e le responsabilità connesse, autorizzato dalla Direttrice / Direttore di Dipartimento e dal Dirigente della struttura competente per la gestione della sicurezza informatica (o delegati).

Altri assegnatari di strumentazione informatica di Ateneo – Soggetti assegnatari di strumentazione informatica di Ateneo o di licenze per l'utilizzo di risorse software, di cui all'art. 2 del presente Regolamento; ad essi spetta l'osservanza del presente regolamento e l'attuazione di azioni proattive volte alla salvaguardia della sicurezza stessa, ivi compresa la segnalazione di eventuali rischi per la sicurezza di cui vengano a conoscenza.

Struttura di monitoraggio ed audit – Il Consiglio di Amministrazione, su proposta del Rettore, può istituire apposita Commissione / Struttura di monitoraggio, controllo o audit dei processi relativi alla sicurezza informatica, volto a verificarne la funzionalità e l'adeguatezza nel tempo.

Incident Response Team ("IRT") – istituito con con D.R. rep. n. 390/2019 del 19.03.2019 che si occupa della strutturazione di un piano di lavori che definisca una nuova versione della procedura di Data Breach, per individuare le minacce, le vulnerabilità e i rischi collegati a tutti gli asset informatici presenti; per prendere precauzioni al fine di proteggere i dati da possibili attacchi; mitigare gli effetti di eventuali violazioni alla rete o ai sistemi informatici.

Amministratori di Sistema (AdS) - individuati ai sensi del Provvedimento dell'Autorità Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008".

4. Sicurezza delle informazioni e dei dati

L'Ateneo definisce i livelli di protezione dei dati e delle informazioni, memorizzati nei propri sistemi, mediante una specifica politica, descritta nel documento *Politica di Classificazione dei Dati*. Tale politica individua le diverse tipologie di dati che possono essere memorizzati all'interno dei sistemi informatici di Ateneo, ed associa a ciascuna di essere il livello di protezione adeguato.

La presente politica opera assumendo il rispetto delle disposizioni per la sicurezza fisica dei locali contenenti archivi informatici, ai sensi delle Leggi in materia di protezione dei dati personali.

L'Ateneo definisce altresì le regole specifiche per la memorizzazione e l'elaborazione dei dati, in base al rispettivo livello di protezione, mediante una specifica politica, descritta nel documento *Politica per la Sicurezza della Rete*.

I dati e i documenti utilizzati nell'attività lavorativa devono essere condivisi secondo le modalità descritte nel documento *Politica di Classificazione dei Dati*. In particolare:

a) i dati a cui è attribuito un livello di protezione superiore al *1-basso*, devono essere salvati e archiviati sugli strumenti designati dall'Ateneo (ad es.: cartelle di rete suddivise per area o competenza e strumenti di condivisione in archivi cloud di ateneo o comunque certificati secondo le vigenti disposizioni nazionali);

b) i dispositivi rimovibili dove memorizzare dati di provenienza dai sistemi di Ateneo (ad es.: chiavette e dischi esterni USB) devono essere utilizzati solo per necessità lavorative e devono essere forniti dall'Ateneo stesso (ovvero, non è possibile utilizzare supporti personali). In particolare, tali dispositivi rimovibili che contengono dati a cui è attribuito un livello di protezione uguale o superiore al livello **2-Medio personali** devono implementare la cifratura in modo da non essere leggibili in caso di furto o smarrimento del supporto. I supporti devono essere custoditi con la massima cura per evitare furto o smarrimento;

c) non è consentito cancellare, senza autorizzazione, dati dell'Ateneo o copiarli su supporti personali, ovvero supporti non dotati delle caratteristiche di sicurezza di cui al punto 2b;

d) non è consentito effettuare trasferimenti di informazioni (ad es. software, dati, etc.) e di documenti concernenti proprietà intellettuale, se non per lo svolgimento delle funzioni istituzionali;

e) la condivisione dei dati con soggetti esterni all'Ateneo è autorizzata solo nell'ambito dell'attività lavorativa e deve seguire standard, protocolli e canali che prevedano la cifratura. In generale tutti gli scambi di dati con l'esterno devono avvenire su canali cifrati per garantire la riservatezza dei dati, quindi ad esempio reti VPN, connessioni HTTPS/ TLS / SFTP, ecc.;

f) non è consentito l'utilizzo di servizi personali di condivisione (ad es.: Google Drive, DropBox, WeTransfer, etc.) per il trattamento di dati nell'ambito delle attività lavorative;

g) non è consentito l'utilizzo di servizi di condivisione dati di Ateneo (ad es. Google Drive) per la memorizzazione di file personali e di file non provenienti da sistemi di Ateneo.

5. Sicurezza dei dispositivi e dei sistemi informatici

5.1 Definizioni

I dispositivi e i sistemi informatici, e più in generale gli strumenti atti ad elaborare informazioni comprendono i dispositivi di proprietà dell'Ateneo, inclusi anche quelli acquistati tramite fondi di ricerca, assegnati al personale, quali, a titolo esemplificativo e non esaustivo:

a. personal computer da tavolo;
b. personal computer portatili;
c. thin-client e postazioni diskless;
d. virtual desktop;
e. tablet e dispositivi palmari;
f. smartphone e telefoni fissi;
g. server di elaborazione e di memorizzazione dati;
h. sistemi di storage indipendenti (ad esempio, Network Attached Storage e similari);
i. stampanti.

5.2 I Responsabili della sicurezza dei dispositivi e dei sistemi informatici

Ciascun dispositivo o sistema informatico è associato al relativo *Responsabile della sicurezza*, al quale è affidato il compito di garantire che tale dispositivo o sistema rispetti le misure di sicurezza stabilite nel presente Regolamento e delle varie politiche cui esso fa riferimento.

I responsabili della sicurezza sono individuati secondo le seguenti modalità:

a) per i dispositivi e i sistemi informatici gestiti dall'Amministrazione, l'individuazione è a cura della struttura incaricata della direzione del sistema informativo, e relativi settori / uffici / ulteriori unità organizzative preposte;

b) per i dispositivi e i sistemi informatici ubicati presso strutture di ricerca, didattica o terza missione, ove non gestiti dall'Amministrazione, è individuato nel Direttore di tale Dipartimento o Struttura. Il Direttore può delegare tale responsabilità a uno specifico soggetto afferente a tale struttura.

Ogni assegnatario di un dispositivo informatico o di asset informatico, anche di tipo software, è responsabile di un utilizzo conforme al presente regolamento e relativi allegati.

5.3 Gestione tecnica della sicurezza dei dispositivi informatici

Presso la Sede Centrale di Ateneo e presso le Strutture Decentrate (Poli, Dipartimenti, Scuole, Centri di Ricerca, ecc.) sono attivati uffici preposti a fornire il supporto tecnico necessario per la messa in sicurezza dei dispositivi e dei sistemi informatici ubicati presso ciascuna sede.

Il compito ciascuno di tali uffici è gestire la sicurezza dei dispositivi e dei sistemi informatici in modo tale da assicurare il rispetto del presente regolamento, agendo direttamente sulle configurazioni software e hardware di tali sistemi, ovvero fornire un adeguato supporto al responsabile della sicurezza degli stessi nel caso in cui lo stesso abbia formalmente richiesto di curarne personalmente la configurazione.

È infatti consentito al personale preposto allo svolgimento di attività di ricerca di amministrare personalmente quei dispositivi e sistemi informatici individuati come necessari per tali attività. Tuttavia tale prerogativa viene concessa al soggetto richiedente (che diviene responsabile della sicurezza di tali dispositivi e/o sistemi) dal Direttore della Struttura di afferenza, dietro approvazione di apposita e motivata istanza che individua analiticamente tali dispositivi e sistemi, sentita la struttura incaricata della direzione del sistema informativo.

L'Ateneo si riserva di limitare, ai dispositivi e/o sistemi gestiti direttamente dai relativi responsabili della sicurezza, gli accessi verso parti della propria infrastruttura ICT individuate a proprio insindacabile giudizio.

5.4 Utilizzo sicuro dei dispositivi informatici

L'utilizzo degli strumenti dell'Ateneo deve essere sempre improntato ai principi di correttezza e liceità.

Ciascun dispositivo o sistema informatico è associato ad uno specifico livello di protezione dei dati da esso offerto (così come indicato nel documento *Politica per la Sicurezza della Rete)*, il quale determinerà le tipologie di dati che potrà memorizzare, elaborare e trasmettere, nonché l'accesso ad altre risorse informatiche collegate alla rete di Ateneo.

È vietato modificare la configurazione hardware e/o software di qualunque dispositivo o sistema informatico e telematico aggiungendo o rimuovendo componenti rispetto alle specifiche previste per la classificazione corrente del di protezione dei dati ad esso assegnato, oppure eludendo o compromettendo i meccanismi di protezione, fatta salve le eccezioni di cui al par. 4.3.

È vietato, in particolare, a titolo esemplificativo e non esaustivo:

- agire deliberatamente per degradare l'operatività dei sistemi e della rete dell'Ateneo e per impedirne l'uso da parte di altri utenti;

- installare, eseguire o diffondere su qualunque computer e sulla rete programmi che possano danneggiare i sistemi o determinare un accesso non autorizzato ai dati (ad es. malware, etc.);
- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare dati di altri utenti;
- utilizzare software che mettano a rischio la sicurezza dei sistemi e la protezione dei dati;
- installare software privo di regolare licenza d'uso in corso di validità;
- utilizzare strumenti dell'Ateneo per la conservazione o la condivisione di materiale per il quale si configuri la violazione della normativa a protezione del diritto d'autore, nonché di materiale pornografico o in qualsiasi modo illecito o lesivo della dignità umana.

5.5 Strumenti di sicurezza

Tutti i dispositivi e i sistemi informatici operanti nell'infrastruttura ICT di Ateneo devono essere dotati di strumenti di aggiornamento automatico dei sistemi operativi, di difesa da malware e di monitoraggio delle anomalie: l'utente non deve in nessun modo intralciare o inibire il funzionamento di questi strumenti, limitandosi a segnalare tempestivamente qualsiasi tipo di problema all'ufficio per il supporto alla sicurezza referente per la struttura di ubicazione del dispositivo o sistema in questione.

L'Ateneo si può avvalere di sistemi di gestione centralizzata dei dispositivi e sistemi informatici al fine di:

- attivare procedure di autenticazione aggiuntive;
- imporre il rispetto delle configurazioni prestabilite e inibirne la modifica;
- inventariare automaticamente l'hardware e il software;
- definire adeguate politiche di backup dei dati;
- aggiornare automaticamente i sistemi operativi e il software;
- attivare procedure di cancellazione remota da utilizzare in caso di smarrimento/furto del dispositivo;
- cifrare automaticamente i dati;
- inibire l'installazione di applicazioni indesiderate;

5.6 Verifiche di sicurezza

L'Ateneo si riserva di effettuare, con adeguata periodicità e frequenza, verifiche atte a valutare la corrispondenza dei dispositivi, delle misure di sicurezza applicate e dei sistemi informatici a livelli adeguati di sicurezza.

Tale verifiche sono estese ed effettuabili anche verso fornitori terzi che operano in qualità di "Responsabili del trattamento dei dati personali" ai sensi dell'articolo 28 del GDPR previa sottoscrizione di specifico accordo per il trattamento dei dati personali. L'Ateneo garantisce la possibilità di effettuare specifiche verifiche ed audit di sicurezza verso i soggetti designati quali responsabili del trattamento grazie all'introduzione di specifiche clausole contrattuali in tal senso inserite all'interno degli accordi per il trattamento dei dati personali sottoscritti.

Tali verifiche potranno comprendere sia attività di semplice scansione delle eventuali vulnerabilità esposte da tali dispositivi e sistemi (*vulnerability scanning*), sia attività di tentativo controllato di intrusione degli stessi (*penetration testing*).

In particolare, saranno sottoposti a penetration testing tutti quei dispositivi o sistemi informatici ubicati all'interno della rete di Ateneo che erogano servizi accessibili dall'esterno di tale rete quali, a titolo esemplificativo e non esaustivo: web server relativi a specifici gruppi di ricerca e/o progetti di ricerca, programmi applicativi, sistemi di archiviazione dati e similari.

Al termine delle attività di verifica della sicurezza di un determinato dispositivo o sistema informatico, sarà inviato al relativo Responsabile della Sicurezza un report che riporta analiticamente le vulnerabilità eventualmente individuate.

Il Responsabile della Sicurezza è tenuto ad adottare le opportune misure atte a eliminare tali vulnerabilità (quali, ad esempio, aggiornamento o disinstallazione di componenti software, modifiche alla configurazione del sistema operativo o delle applicazioni, ecc.) entro un termine perentorio individuato dall'ufficio per il supporto alla sicurezza referente per la struttura di ubicazione del dispositivo o sistema in questione.

La responsabilità di compromissione della sicurezza dell'infrastruttura ICT di Ateneo e dei dati e/o informazioni in essa memorizzata, dovuta al mancato adeguamento di dispositivi e sistemi informatici alle misure di sicurezza individuate dal presente regolamento e dalle politiche cui esso fa riferimento, ricade interamente sui Responsabili della Sicurezza di tali dispositivi e sistemi.

L'Ateneo si riserva, nelle more della risoluzione delle vulnerabilità individuate per un determinato dispositivo o sistema informatico, di disabilitarne la connessione alla rete di Ateneo.

5.7 Controllo, monitoraggio e registrazione

L'Ateneo è tenuto ai controlli relativo all'accesso, l'utilizzo e il funzionamento dei servizi ICT da esso erogati, sia tramite sistemi di monitoraggio automatico centralizzato, sia tramite agenti volti a salvaguardare il buon funzionamento dei dispositivi, e la protezione da minacce informatiche (quali a titoli esemplificativo antivirus), che operano anche nell'ambito di azioni di manutenzione ciclica dei dispositivi.

L'attività di cui al periodo precedente si esplica anche attraverso il mantenimento di registri delle attività (log) di vario tipo, inerenti i servizi, nel rispetto della normativa vigente di trattamento dei dati personali (definiti nel successivo Par. 5.10, che dettaglia le fonti da cui si raccolgono i log e le modalità di gestione).

Tali controlli sono finalizzati a:

- ottemperare alla normativa cogente in materia protezione dei dati;
- rispondere ad eventuali richieste dell'autorità giudiziaria;
- garantire la sicurezza dei servizi anche tramite sistemi per la verifica delle intrusioni informatiche (IDS);
- verificare la corretta gestione dei flussi di dati e informazioni;
- implementare l'inventario delle risorse in rete e dei software utilizzati;

- elaborare statistiche d'uso, gestendo il dato in forma anonima, relative ai sistemi informatici;
- svolgere attività relative a modifiche tecniche/operative;
- verificare la corretta configurazione dei sistemi;
- raccogliere e preservare le evidenze forensi a supporto di ogni eventuale azione legale che coinvolga l'Ateneo;
- contrastare utilizzi impropri e/o illeciti e più in generale contrari alla politica d'uso accettabile, al presente disciplinare ed alla normativa vigente;
- monitorare l'uso delle credenziali rilasciate agli utenti.

È escluso ogni utilizzo dei dati raccolti per fini diversi da quelli sopra citati, in particolare per qualunque forma di controllo a distanza degli utenti/ monitoraggio dell'attività lavorativa del singolo individuo.

L'accesso ai registri delle attività (log) è consentito solo al personale autorizzato e riguarda in primo luogo dati aggregati non riferibili a un singolo utente. L'accesso ai dati di utilizzo di un singolo utente, laddove necessario, avviene per giustificati motivi. In nessun caso sono ammessi controlli prolungati e costanti.

Alcune attività (ad es. amministratori di sistema) sono raccolte e gestite in adempimento alla normativa vigente.

5.8 Accesso remoto all'infrastruttura ICT di Ateneo

L'accesso remoto all'infrastruttura ICT di Ateneo viene garantito attraverso l'uso di un canale di comunicazione cifrato VPN (Virtual Private Network), che viene attivato mediante l'uso di specifico software (client VPN) installato sui dispositivi abilitati, ovvero di altri canali che consentano la cifratura delle comunicazioni.

L'utente utilizzerà le credenziali personali di accesso da gestire secondo le disposizioni del presente regolamento. L'Ateneo potrebbe modificare le modalità tecniche di collegamento privilegiando altre soluzioni equivalenti sotto il profilo della sicurezza come l'utilizzo di desktop virtuali forniti dall'Ateneo.

L'utente che esegue l'accesso remoto deve assicurarsi che il computer dal quale si effettua la connessione rispetti le disposizioni stabilite dal presente Regolamento e/o dalle Politiche cui esso fa riferimento.

Il presente regolamento, opera in coerenza con le "Disposizioni per lo svolgimento della prestazione lavorativa a distanza nell'Università del Piemonte Orientale" di cui al Decreto Rettorale 1339/2022 del 12 agosto 2022 e ss.mm.ii, applicabili al Personale Tecnico, Amministrativo e Bibliotecario.

5.9 Gestione sicura delle credenziali di autenticazione

L'accesso all'infrastruttura ICT di Ateneo è regolato dal sistema di autenticazione per i servizi informatici, le cui credenziali sono costituite da un identificativo (detto anche username o user id) e da una password, ovvero da ulteriori sistemi di autenticazione, come previsti dalla normativa vigente. L'identificativo generalmente coincide con l'indirizzo email universitario dell'utente.

Tutte le credenziali sono strettamente personali, e ogni utente è responsabile della loro custodia e riservatezza, avendo cura che non vengano utilizzate in modo improprio. La cessione a terzi delle proprie credenziali costituisce violazione del presente regolamento.

La password scelta dall'utente deve rispettare i criteri di robustezza e sicurezza indicati nell'allegato *Politica dei profili utente e delle password*.

Al di fuori dei servizi compresi nella gestione con single sign-on, l'utente deve scegliere password differenti per ogni sistema o applicativo a cui ha accesso, compresi eventuali servizi di terze parti a cui deve registrarsi con un profilo di posta elettronica fornito dall'Ateneo. Le credenziali non devono mai essere riutilizzate.

Le politiche di Ateneo richiedono una scadenza periodica delle credenziali di accesso; l'utente verrà avvisato in modo automatico della necessità di scegliere una nuova password, rispettando sempre i criteri definiti in precedenza.

Nel caso si sospetti che la propria password abbia perso la caratteristica della segretezza si deve procedere ad una modifica immediata della stessa. Analogamente, qualora l'utente venga a conoscenza di credenziali violate di un altro utente, è tenuto a notificarlo immediatamente all'ufficio per il supporto alla sicurezza referente per la struttura di ubicazione del dispositivo o sistema in questione.

Per i servizi non integrabili nel sistema di autenticazione centralizzata, ovvero i dispositivi e i sistemi informatici gestiti direttamente dal relativo responsabile della sicurezza, è previsto comunque l'uso di credenziali locali rilasciate da tale responsabile, le quali dovrebbero essere gestite con criteri allineati all' allegato *Politica dei profili utente e delle Password*.

5.10 Gestione dei log

La gestione dei log da parte dell'Ateneo è necessaria per assicurare il rispetto della normativa a tutela dei dati personali, poiché consente di ricostruire l'attività di un sistema informatico e individuare eventuali responsabilità in caso di errore, violazioni di legge e data breach (art. 33 comma 3 del Regolamento UE 2016/679). Il principio di responsabilità (art. 5 comma 2 del Regolamento UE 2016/679) introduce l'obbligo, in capo al Titolare del trattamento, di dimostrare il rispetto della normativa decidendo autonomamente modalità, garanzie e limiti del trattamento dei dati personali, in considerazione del contesto operativo in cui l'Ente opera. Da una parte, quindi, i titolari del trattamento non solo devono compiere tutte le attività necessarie per la salvaguardia degli interessati, ma devono anche precostituirsi le prove degli adempimenti in caso di ispezioni da parte delle autorità competenti.

I log sono devono essere conservati e mantenuti in modo appropriato per prevenire eventuali perdite di informazioni o la possibile compromissione da parte di intrusi. La conservazione dei log deve inoltre rispettare i requisiti normativi e fornire le informazioni necessarie per attività forensi e di risposta agli incidenti.

I log devono essere gestiti in modo centralizzato e accessibili alla Struttura deputata al coordinamento della sicurezza Informatica di cui all'art. 3, per poter effettuare una correlazione anche automatizzata delle informazioni in essi contenuti. al fine di soddisfare i requisiti normativi e

fornire le sufficienti informazioni necessarie per le attività forensi, di risposta agli incidenti e di analisi di data breach.

6. Gestione degli incidenti di sicurezza

6.1 Tracciatura degli incidenti di sicurezza

Gli incidenti di sicurezza vengono tracciati su apposito registro secondo modalità previste nel documento *Politica di gestione degli incidenti di sicurezza*.

Tutti gli utenti hanno l'obbligo di segnalare tempestivamente, all'ufficio per il supporto alla sicurezza referente per la struttura di ubicazione del dispositivo o sistema coinvolto, ogni anomalia nel funzionamento del sistema informativo di Ateneo o qualsiasi comportamento volontario o accidentale, anche di terzi esterni all'Ateneo, che possa esporre i dati ivi memorizzati al rischio di furto, perdita o modifica non autorizzata. Nel caso si sospetti una compromissione degli strumenti informatici da parte di un malware o di un soggetto esterno all'Ateneo, questa deve essere segnalata prima possibile alla struttura ICT di riferimento.

In caso sospetta compromissione della sicurezza occorre attenersi alla seguente procedura:

- non spegnere per nessuna ragione il dispositivo (ad es.: PC, Smartphone, etc.);
- interrompere il collegamento alla rete dati (ad es. staccare il cavo di rete, disabilitare il WIFI, mettere il dispositivo in modalità "aereo". etc.);
- non cancellare nulla dal dispositivo perché i dati raccolti possono essere fondamentali per l'analisi e la risoluzione dell'incidente;
- segnalare immediatamente l'anomalia alla struttura ICT di riferimento come potenziale incidente di sicurezza e attenersi alle istruzioni che verranno impartite.

6.2 Limitazione dell'utilizzo delle risorse

A seguito della rilevazione di un incidente di sicurezza informatica e/o per rispondere a richieste dell'Autorità Giudiziaria e in considerazione della possibilità di dover rispondere ad eventuali obblighi giuridici di rispetto della catena di custodia volta a preservare evidenza di incidenti particolarmente gravi, l'Ateneo può:

- limitare o impedire l'uso del dispositivo (ad es.: esclusione dalla rete di Ateneo) o l'accesso ai servizi di Ateneo;
- chiedere la consegna del dispositivo per il tempo necessario a compiere le attività di analisi e risoluzione dell'incidente;
- imporre il ripristino sicuro e verificato dalla struttura ICT di riferimento del dispositivo come condizione necessaria per l'accesso ai servizi di Ateneo.

7. Glossario dei termini

Account: Un account è un'identità digitale che consente l'accesso a un sistema informatico, a un'applicazione o a una risorsa online. Di solito è protetto da credenziali di accesso, come nome utente e password.
Algoritmi di crittografia: Gli algoritmi di crittografia sono procedure matematiche utilizzate per crittografare e decrittografare dati. Questi algoritmi rendono i dati incomprensibili a meno che non si possieda la chiave di decrittazione corretta.
Asset: Gli asset sono risorse digitali di valore, come dati, software, hardware o proprietà intellettuale, che possono essere gestiti e protetti da un'organizzazione.
Backup: Un backup è una copia di sicurezza dei dati critici memorizzati su un dispositivo o su un sistema. I backup vengono utilizzati per ripristinare i dati in caso di perdita, danneggiamento o eliminazione accidentale.
Banda di trasmissione di dati: La banda di trasmissione di dati si riferisce alla capacità massima di trasferimento dati di una connessione di rete, espressa in bit per secondo (bps) o in unità di misura più grandi come kilobit, megabit o gigabit al secondo.
Cloud: Il cloud computing è un modello di erogazione di servizi informatici tramite Internet, che consente l'accesso on-demand a risorse informatiche condivise, come server, archiviazione, database, applicazioni e altro ancora. Gli archivi cloud sono servizi di memorizzazione online che consentono agli utenti di archiviare, gestire e condividere dati su server remoti attraverso Internet.
Protocolli HTTPS/TLS/SFTP: Sono protocolli di comunicazione sicuri utilizzati per proteggere la trasmissione di dati su Internet. HTTPS (Hypertext Transfer Protocol Secure) viene utilizzato per siti web, TLS (Transport Layer Security) è un protocollo di crittografia utilizzato per garantire la privacy e l'integrità dei dati scambiati su una rete, mentre SFTP (Secure File Transfer Protocol) è un protocollo per il trasferimento sicuro di file su una rete.
Cookie: I cookie sono piccoli file di testo memorizzati sul computer di un utente quando visita determinati siti web. I cookie vengono utilizzati per memorizzare informazioni sulle preferenze dell'utente, tracciare il comportamento di navigazione e personalizzare l'esperienza online.
Credenziali di accesso: Le credenziali di accesso sono le informazioni utilizzate per autenticare l'identità di un utente e consentire l'accesso a un sistema, a un'applicazione o a una risorsa protetta. Di solito includono un nome utente e una password, ma possono anche includere altri metodi di autenticazione, come le impronte digitali o i codici OTP (One-Time Password).
Crittografia (hash salted): La crittografia hash salted è una tecnica di crittografia che prevede l'aggiunta di una stringa casuale (salt) ai dati prima di crittografarli con una funzione hash. Questo rende più difficile per gli aggressori eseguire attacchi di forza bruta o di dizionario per decifrare i dati.
Data Breach: È una violazione di dati personali; si verifica quando informazioni sensibili vengono fruite, divulgate, rubate o utilizzate in modo non autorizzato. Questo può accadere a causa di vulnerabilità di sicurezza, errori umani o attacchi informatici.
Dato: Un dato è una rappresentazione simbolica di fatti, concetti o istruzioni in una forma adatta per l'elaborazione da parte di un computer. I dati possono essere di diversi tipi, tra cui testo, numeri, immagini, audio, video, ecc.

Deidentificazione: La deidentificazione è il processo di rimozione o alterazione delle informazioni personali da un insieme di dati in modo che non possano essere associate a un individuo specifico senza l'uso di informazioni aggiuntive.
Dispositivi rimovibili: I dispositivi rimovibili sono dispositivi di archiviazione esterni, come chiavette USB, schede di memoria e dischi rigidi esterni, che possono essere collegati e rimossi da un computer o da altri dispositivi.
DMZ: La DMZ (Demilitarized Zone) è una zona di rete intermedia tra una rete interna sicura e una rete esterna non attendibile, utilizzata per ospitare servizi pubblici, come server web o server di posta, che devono essere accessibili dall'esterno, ma separati dalla rete interna.
ICT: ICT (Information and Communication Technology) è un termine generico che si riferisce a tutte le tecnologie utilizzate per la comunicazione e l'elaborazione delle informazioni, inclusi computer, reti, software, internet, telecomunicazioni e altre tecnologie digitali.
Indirizzo IP: Un indirizzo IP (Internet Protocol address) è un identificatore numerico assegnato a ogni dispositivo connesso a una rete informatica che utilizza il protocollo Internet per la comunicazione.
Informazione: In informatica, un'informazione è un dato che è stato elaborato, organizzato o interpretato in modo significativo per fornire conoscenza o supportare decisioni.
Intranet: Un'intranet è una rete informatica privata basata su tecnologie Internet, utilizzata da un'organizzazione per condividere risorse, informazioni e strumenti di collaborazione all'interno dell'azienda.
Log di sistema: I log di sistema sono file di registro che registrano eventi, attività e errori che si verificano su un sistema informatico, come un server o un computer, e sono utilizzati per il monitoraggio, la diagnostica e l'analisi.
Malware: Il malware è un termine generico che si riferisce a software malevolo progettato per danneggiare, infiltrarsi o compromettere un sistema informatico o una rete, inclusi virus, worm, trojan, ransomware e spyware.
Modalità "aereo": La modalità "aereo" è una modalità di funzionamento su dispositivi mobili, come smartphone o tablet, che disattiva tutte le connessioni wireless, come Wi-Fi, Bluetooth e reti cellulari, per ridurre l'interferenza durante i voli.
Penetration testing: Il test di penetrazione, è un'attività di sicurezza informatica che consiste nel simulare un attacco informatico contro un sistema, una rete o un'applicazione al fine di identificare e correggere vulnerabilità di sicurezza.
Pseudonimizzazione: La pseudonimizzazione è una tecnica di protezione dei dati che coinvolge la sostituzione delle informazioni identificative con pseudonimi o codici univoci per ridurre il rischio di identificazione degli individui.
Registri delle attività (log): Vedi "Log di sistema".
Risorse di calcolo: Le risorse di calcolo si riferiscono alle capacità di elaborazione disponibili su un sistema informatico, come CPU, memoria e capacità di archiviazione.
Server di elaborazione e di memorizzazione dati: I server di elaborazione e di memorizzazione dati sono sistemi informatici dedicati al trattamento e all'archiviazione di dati, spesso utilizzati in ambienti aziendali per gestire informazioni rilevanti e critiche.

Sicurezza informatica: La sicurezza informatica è il campo che si occupa di proteggere i sistemi informatici, le reti e i dati da accessi non autorizzati, danni o intrusioni.
Single sign-on: Il single sign-on è un sistema di autenticazione che consente agli utenti di accedere a più sistemi o applicazioni utilizzando un'unica identità di accesso, riducendo la necessità di inserire ripetutamente le credenziali.
Sistema pubblico di connettività (Italia): Il Sistema Pubblico di Connettività (in acronimo SPC) è la rete che collega tra loro tutte le pubbliche amministrazioni italiane, consentendo loro di condividere e scambiare dati e risorse informative.
Sistemi di autenticazione: Vedi "Single sign-on".
Sistemi di storage: I sistemi di storage sono dispositivi o servizi utilizzati per archiviare, gestire e accedere ai dati, come dispositivi di storage di rete (NAS) e soluzioni cloud storage.
Sistemi Operativi: Un sistema operativo è un insieme di software che gestisce le risorse hardware e fornisce servizi di base per l'uso del computer. Tra le sue funzioni principali vi sono la gestione dei file, la gestione della memoria, la gestione dei dispositivi, la gestione delle interfacce utente e l'esecuzione di programmi.
Sistemi per la verifica delle intrusioni informatiche (IDS): I sistemi per la verifica delle intrusioni informatiche (IDS) sono dispositivi o software progettati per rilevare e segnalare attività sospette o comportamenti anomali su una rete informatica.
Smartphone e telefoni fissi: Gli smartphone sono dispositivi mobili avanzati che combinano funzionalità di telefonia con capacità di elaborazione, memorizzazione e connettività Internet. I telefoni fissi sono dispositivi utilizzati per le comunicazioni vocali tramite linee telefoniche fisse.
Tablet e dispositivi palmari: I tablet sono dispositivi portatili simili a computer con uno schermo touch-screen, utilizzati principalmente per la navigazione web, la lettura di e-book, la visualizzazione di media e l'utilizzo di applicazioni. I dispositivi palmari sono dispositivi di dimensioni più piccole, come organizer e PDA (Personal Digital Assistant).
Thin-client e postazioni diskless: Le thin-client sono dispositivi informatici con risorse di elaborazione minime progettati per accedere e utilizzare applicazioni e dati memorizzati su server remoti. Le postazioni diskless sono computer che operano senza un disco rigido locale, accedendo invece a un sistema operativo e a dati da risorse di rete.
USB: USB (Universal Serial Bus) è uno standard di connessione per collegare dispositivi periferici, come tastiere, mouse, stampanti, unità di archiviazione esterne e dispositivi mobili, a un computer o a altri dispositivi.
Virtual desktop: Un virtual desktop è un'istanza di sistema operativo ospitata ed eseguita su un server remoto e accessibile da un dispositivo client tramite una connessione di rete, consentendo agli utenti di accedere alle proprie applicazioni e dati da qualsiasi luogo.
VPN: Una Virtual Private Network (VPN) è una rete privata virtuale che crea una connessione crittografata e sicura su una rete pubblica, come Internet, consentendo agli utenti di accedere in modo sicuro a risorse di rete remote.
Vulnerability scanning: La scansione delle vulnerabilità è il processo di individuazione e valutazione di potenziali vulnerabilità di sicurezza su un sistema informatico o una rete, al fine di identificare e correggere le aree a rischio.

Web server: Un web server è un software o un'applicazione che fornisce contenuti web agli utenti tramite il protocollo HTTP su Internet.
WI-FI: Il Wi-Fi è una tecnologia di rete wireless che consente agli utenti di connettersi a Internet e alle reti locali tramite onde radio, senza l'uso di cavi.

8. Allegati

Il presente regolamento è integrato dai seguenti allegati che ne costituiscono parte integrante

1. All. 1 - Politica per la Sicurezza della Rete
2. All. 2 - Politica di Classificazione dei Dati
3. All. 3 - Politica dei profili utenti e delle password
4. All. 4 - Politica per la gestione degli incidenti di sicurezza informatica[1]

[1] In fase di prima approvazione del regolamento per tale politica si fa riferimento alla prassi definita alla pagina https://www.uniupo.it/it/ateneo/regolamenti-trasparenza-sindacati/protezione-dei-dati-personali, con particolare riferimento alle funzioni dell'Incident Response Team.

Politica per la sicurezza della rete di Ateneo

Sommario

1. Scopo del documento

Lo scopo di questo documento è definire l'architettura di riferimento per la suddivisione della rete di Ateneo in aree omogenee, e delle policy che specificano le regole di accesso a tale rete, al fine di:

1. creare una struttura logica che consenta di compartimentalizzare gli accessi da parte di un dispositivo o sistema connesso alla rete di Ateneo verso gli altri dispositivi o sistemi connessi a tale rete, al fine di garantire un livello adeguato di protezione di sistemi e dati;
2. definire le regole che specificano l'appartenenza di ciascun dispositivo o sistema alle varie aree in cui è suddivisa la rete di Ateneo.

2. Ambito di applicazione

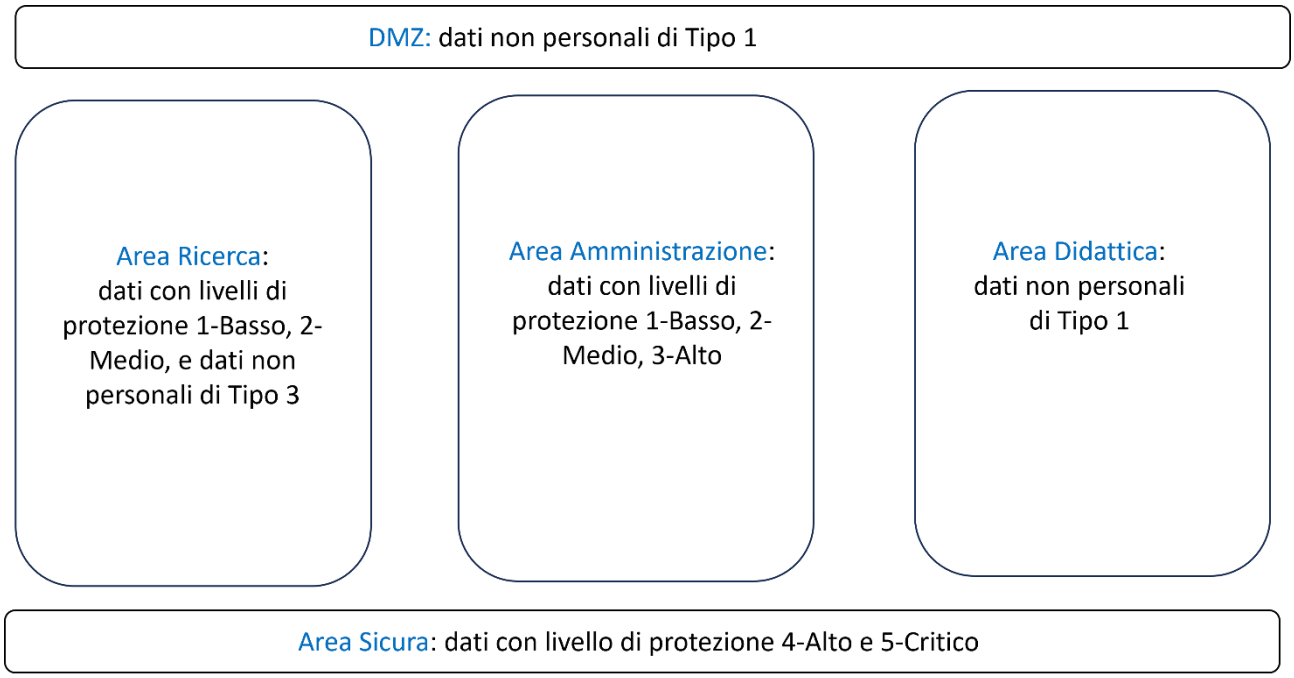
La politica descritta in questo documento si applica a qualsiasi dispositivo o sistema informatico connesso alla rete di Ateneo, quali, a titolo esemplificativo e non esaustivo:

a. personal computer da tavolo;
b. personal computer portatili;
c. thin-client e postazioni diskless;
d. smartphone e tablet;
e. server di elaborazione e di memorizzazione dati;
f. sistemi di storage indipendenti (ad esempio, Network Attached Storage e similari);
g. altri sistemi connessi alla rete di Ateneo quali dispositivi IoT.

3. Strutturazione della rete di Ateneo

La rete di Ateneo è suddivisa in 5 aree, schematicamente rappresentate nella figura sottostante, omogenee tra loro dal punto di vista del dominio applicativo in cui si trovano a operare i dispositivi e i sistemi connessi a ciascuna di esse.

La filosofia di base sottesa alla suddivisione della rete in aree prevede che i dispositivi e i sistemi connessi ad una qualunque area non possano comunicare direttamente con dispositivi e sistemi connessi ad aree caratterizzate da un livello di sicurezza più alto rispetto a quello del primo dispositivo. In questo modo, un'eventuale compromissione di un dispositivo o di un sistema non potrà impattare su dispositivi e sistemi connessi ad altre aree, pur tuttavia potendo impattare sui dispositivi e sistemi connessi alla stessa area.



Come può apprezzarsi dalla figura sopra riportata, ciascuna area è contraddistinta da una denominazione (corrispondente al dominio applicativo ad essa relativo), e dall'individuazione dal livello di protezione caratterizzante i dati che possono essere memorizzati in essa, così come definito nella "Policy di classificazione dei dati".

A ciascuna di tali aree saranno connessi i dispositivi e i sistemi in base alle seguenti regole di classificazione:

1. DMZ: in tale area saranno collocati dispositivi e sistemi che necessitano di essere raggiungibili dall'esterno della rete di Ateneo, quali ad esempio quelli utilizzati per erogare servizi di vario genere o la cui gestione è demandata a gruppi di ricerca che li utilizzano per le proprie attività sperimentali e/o progettuali. Nella DMZ possono essere memorizzati esclusivamente dati caratterizzati dal livello di protezione 1-Basso.
2. Area Ricerca: in tale area saranno collocati dispositivi e sistemi utilizzati per attività di ricerca che non richiedono di essere raggiungibili dall'esterno della rete di Ateneo (ad esempio, computer fissi/portatili di dottorandi, contrattisti, docenti, ecc.). Su tali sistemi e dispositivi potranno essere memorizzati esclusivamente dati caratterizzati dai livelli di protezione 1-Basso e 2-Medio, nonché dati non personali di Tipo 3 (con livello di protezione 3-Alto)

3. Area Amministrazione: in tale area saranno collocati dispositivi e sistemi utilizzati per l'attività amministrativa, e potranno essere memorizzati esclusivamente dati caratterizzati dai livelli di protezione 1-Basso, 2-Medio e 3-Alto.
4. Area Didattica: in tale area saranno collocati dispositivi e sistemi utilizzati per attività didattiche, e potranno essere memorizzati esclusivamente dati non personali di Tipo 1 (caratterizzati dal livello di protezione 1-Basso).
5. Area Sicura: quest'area è dedicata alla memorizzazione e gestione di dati caratterizzati dai livelli di protezione 4-Alto e 5-Critico.

4. Regole per l'accesso di dispositivi e sistemi alle aree della rete

Il principio di base adottato per l'accesso di un determinato dispositivo o sistema ad una specifica area della rete di Ateneo è il rispetto delle prescrizioni previste dalla Circolare AGID n. 2/2017 riportante le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" e ss.mm.ii..

In particolare, l'accesso di un dispositivo o un sistema ad una determinata area della rete richiede che tale dispositivo o sistema rispetti le misure previste per il livello di protezione dei dati memorizzati in tale area, così come definiti nella "Policy per la classificazione dei dati".

Ciascun dispositivo o sistema sarà certificato, mediante un'apposita procedura, con il livello di protezione da esso offerto, e potrà accedere ad aree per le quali il suo livello di protezione corrisponda al livello di protezione più elevato per i dati contenuti in tale area.

Nel caso in cui un dispositivo o sistema, anche portatile o trasportabile, abbia necessità di accedere a più aree diverse, in momenti differenti o anche contemporaneamente, il suo livello di protezione dovrà corrispondere a quello più elevato tra tutti i dati memorizzati in tali aree.

Per quanto riguarda l'Area Sicura, ad essa potranno essere connessi esclusivamente dispositivi o sistemi non portatili o trasportabili. L'eventuale necessità di uso dei dati memorizzati in tale area potrà essere soddisfatta mediante creazione di una copia degli stessi su un supporto di memoria criptato, e uso di tali dati su un dispositivo o sistema certificato con livello di protezione pari ad almeno 4-Molto Alto.

Politica di classificazione dei dati

Sommario

1. Scopo del documento

Lo scopo di questo documento è fornire un metodo di classificazione dei dati trattati dall'Università del Piemonte Orientale in base al loro valore e criticità per l'organizzazione, con l'obiettivo di individuare le misure di protezione più adeguate.

2. Ambito di applicazione

La politica descritta in questo documento si applica a qualsiasi forma di dati, inclusi i dati digitali memorizzati su qualsiasi tipo di supporto, che siano soggetti a trattamento da parte di dipendenti, collaboratori dell'Ateneo e/o persone o società autorizzate al trattamento stesso.

3. Classificazione delle tipologie di dati

I dati trattati si distinguono in:

1. Dati personali;
2. Dati non personali.

3.1 Dati personali

Per **dato personale** si intende qualsiasi informazione riconducibile, in modo univoco, a una persona identificata o identificabile.

Anche **le diverse informazioni che, raccolte insieme, possono portare all'identificazione di una determinata persona** costituiscono i dati personali. Ad esempio, un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale costituiscono, nel loro insieme, un dato personale.

I dati personali sottoposti a **cifratura, pseudonimizzazione** ovvero altra forma di **deidentificazione** prevista dalla normativa vigente**,** ma che possono essere utilizzati per reidentificare una persona, rimangono dati personali. Esempi di dati personali:

- nome e cognome;
- indirizzo di casa;
- indirizzo e-mail come nome.cognome@azienda.com;
- numero della carta d'identità;
- dati sulla posizione (ad es. la funzione di posizionamento su un telefono cellulare);
- indirizzo IP;
- ID cookie;
- Ecc…

3.1.1 Categorie particolari di dati personali

Costituiscono categorie **particolari** di dati personali quelli che rivelino l'**origine razziale o etnica**, le **opinioni politiche**, le **convinzioni religiose o filosofiche**, o l'**appartenenza sindacale**, nonché i **dati genetici**, i **dati biometrici** intesi a identificare in modo univoco una persona fisica, i **dati relativi alla salute** o alla vita sessuale o **all'orientamento sessuale** della persona.

Anche i dati personali relativi alle **condanne penali e ai reati** o a connesse misure di sicurezza sono da considerarsi particolari e possono essere trattati soltanto sotto il controllo dell'autorità pubblica, o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

3.2 Dati non personali

I **dati non personali** sono dati che **non identificano né rendono identificabile una persona fisica.** Esempi di dati non considerati personali:

- numero di iscrizione al registro delle imprese di una società;
- indirizzo e-mail impersonale come info@azienda.com;
- dati resi anonimi in modo irreversibile;
- dati statistici;
- dati aggregati;
- brevetti;
- piani aziendali;
- bilanci;
- ecc.

Partendo da queste due categorie sono state definite dieci tipologie di dati ognuna con un livello di protezione adeguato al rischio associato ai dati trattati dall'Ateneo e memorizzati su risorse informatiche interne all'Ateneo con riferimento a dispositivi di proprietà dell'Ateneo stesso.

Le tipologie di dati elencate di seguito sono in ordine di rilevanza crescente sotto il profilo dell'impatto in caso di perdita di riservatezza, disponibilità e integrità dei dati.

Il livello di protezione associato a ciascuna tipologia di dato può assumere uno di questi cinque valori: basso, medio, alto, molto alto, critico. I livelli di protezione, descritti in un paragrafo successivo, sono definiti da un insieme di strumenti, procedure e sistemi di controllo adeguati a quel livello.

Tipo di dato	Descrizione	Livello di protezione	Esempio
Dati non personali tipo 1	Sono dati non personali solitamente destinati alla divulgazione pubblica, specialmente attraverso applicativi web propri o di terze parti.	1 – Basso	• Bandi, • informazioni sull'ente, • dati aggregati, • mappe, • …
Dati personali tipo 1	Rientrano in questa categoria i dati personali che a seguito degli obblighi di trasparenza applicabili all'ente, sono oggetto di pubblicazione sul portale di Ateneo e altre sedi pubblicamente accessibili.	1 – Basso	• Nome e cognome di assegnisti o collaboratori, • curricula e compensi delle figure apicali, • …
Dati non personali tipo 2	Rientrano in questa categoria i dati che generalmente non sono pubblicabili o accessibili senza un controllo dell'identità di chi li consulta. La perdita di riservatezza, integrità o disponibilità di questi dati potrebbe avere un impatto negativo moderato sulla missione aziendale in termini di sicurezza, reputazione o sotto l'aspetto economico-finanziario.	2 – Medio	• Dati dei processi aziendali, • materiale didattico per gli studenti iscritti, • contenuti didattici a pagamento, • …
Dati personali tipo 2	Rientrano in questa categoria i dati personali per i quali non è prevista la pubblicazione.	2 – Medio	• Documenti d'identità, • indirizzo del domicilio privato, • numero di cellulare • …

Dati non personali tipo 3	Rientrano in questa categoria i dati la cui protezione è richiesta per legge o da regolamenti di categoria. Dalla perdita di riservatezza, integrità o disponibilità dei dati o del sistema potrebbe derivarne un impatto negativo significativo sulla missione aziendale in termini di sicurezza, reputazione o sotto l'aspetto economico finanziario.	3 – Alto	• Risultati di ricerche non ancora pubblicati, • pianificazione del budget, • bilanci, • strategie aziendali, • proprietà intellettuale, • …
Dati particolari (ad esclusione di quelli riferibili a tipologie successive)	Sono dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare l'orientamento sessuale.	3 – Alto	• Adesione sindacale, • adesione a organizzazioni universitarie, • …
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali i dati dell'immagine facciale o i dati dattiloscopici.	4 – Molto alto	• Immagini del volto, • impronte digitali, • timbro vocale, • qualsiasi elemento fisico idoneo ad essere letto e interpretato da programmi di riconoscimento automatizzato, • …
Dati sanitari	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.	4 – Molto alto	• Temperatura corporea, • patologie pregresse o in corso, • referti medici, • …

Dati giudiziari	I dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o indagato. Il Regolamento UE 2016/679 (art. 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza. In particolare, rientrano in questa categoria i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.	4 – Molto alto	• Provvedimenti penali di condanna definitivi, • libertà condizionale, • il divieto od obbligo di soggiorno, le misure alternative alla • detenzione, • • …
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che conferiscono informazioni univoche sulla fisiologia di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.	5 – Critico	• Risultati di esami genetici, • Risultati di test pre-sintomatici o predittivi, • …

4. Livelli di protezione dei dati

Per proteggere i dati con le adeguate misure di sicurezza, sono stati definiti dei livelli di protezione in termini di strumenti informatici, procedure e sistemi di controllo.

Livello di protezione 1 – Basso

Strumenti
Portali web e applicazioni senza autenticazione e cifratura delle informazioni in transito

Backup su dispositivi di Ateneo o specificamente individuati mediante contratti di servizi esterni

Livello di protezione 2 – Medio

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Portali web e applicazioni con autenticazione e cifratura delle informazioni in transito
Supporti mobili, ove funzionalmente richiesti per l'espletamento delle attività istituzionali, con cifratura
Backup (cfr. punto precedente)

Livello di protezione 3 – Alto

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
File server di Ateneo o altra risorsa cloud di Ateneo certificata in base alle disposizioni vigenti, ovvero altre risorse, appositamente individuate con specifiche deroghe rilasciate sulla base di richieste motivate, autorizzate dall'Organo competente, ai sensi art. 4.2 Regolamento.
Backup su dispositivi di Ateneo centralizzati o specificamente individuati mediante contratti di servizi esterni

Procedure
Accesso ai dati solo a un elenco individuato di autorizzati

Livello di protezione 4 – Molto alto

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti

Applicazioni con algoritmi di crittografia forte per le informazioni in transito e basi di dati cifrate
Sistemi di posta elettronica con cifratura dei messaggi
Cifratura dei sistemi di backup previsti al livello 3
Il software utilizzato deve avere analisi con cadenza regolare delle vulnerabilità e aggiornamento continuo

Livello di protezione 5 – Critico

Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Sistemi ICT certificati e applicazioni certificate per la gestione di dati genetici

Se l'attuazione delle suddette configurazioni dovesse incontrare limiti di piena applicabilità per disposizioni regolatorie previste da specifiche normative comunitarie o nazionali, ovvero per vincoli tecnici oggettivi, si provvederà ad applicare il massimo livello di sicurezza possibile, compatibilmente con tali limitazioni.

5. Classificazione dei dati

La classificazione dei dati di cui alla suddetta Sezione 3 è conforme alla gestione dei registri di trattamento dati di cui all'30 del Regolamento (EU) n. 679/2016 e s.s.m.m.i.i..

6. Riferimenti

Elenco dei documenti utilizzati e risorse utili per la comprensione o l'approfondimento.

Nome	Contenuti e indirizzi
Regolamento UE 2016/679 (GDPR)	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/6264597*
"Codice in materia di protezione dei dati personali" D.lgs. 30 giugno 2003, n.196	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/9042678*
Misure Minime di Sicurezza ICT	*https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict*

Regolamento d'Ateneo sul trattamento dei dati personali	*https://www.uniupo.it/it/ateneo/regole-trasparenza-sindacati/normativa/regolamento-di-ateneo-lattuazione-delle-norme-materia-di-protezione-dei-dati-personali*
Center for Internet Security (CIS)	*https://www.cisecurity.org/*

UNIVERSITÀ DEL PIEMONTE ORIENTALE

Politica dei profili utente e delle password

Sommario

1. Scopo del documento

Lo scopo di questo documento è definire i livelli minimi di sicurezza da applicare alla gestione delle credenziali di accesso degli utenti di Ateneo (di seguito anche account), con particolare riferimento alle caratteristiche della password.

Il documento definisce inoltre i criteri generali da adottare per il dimensionamento delle cartelle (directory) personali e di gruppo contenenti i dati degli utenti.

2. Ambito di applicazione

La presente politica si applica d'ufficio a tutte le credenziali di accesso ai sistemi di Ateneo rilasciate agli utenti. L'elenco delle tipologie di utenti sono definite, nell'art. 2 del Regolamento di Ateneo per la sicurezza informatica, di cui la presente Politica costituisce parte integrante.

3. Principi fondamentali per la creazione e gestione delle password

Al fine di ridurre i rischi di compromissione dei sistemi informatici dell'Ateneo sono adottati i seguenti principi fondamentali relativi alla creazione, gestione e protezione delle credenziali, volti a fornire un approccio completo ed integrato rispetto alla sicurezza delle password.

- **Lunghezza e Complessità** - Le password devono essere lunghe e complesse per resistere agli attacchi informatici. L'utente adotta password di almeno 10 caratteri per utenze standard e 15 per quelle amministrative (amministratori di sistema), includendo almeno tre fra i seguenti requisiti di complessità della password stessa:
    - almeno una lettera maiuscola;
    - almeno una lettera minuscola;
    - almeno un numero;
    - almeno un carattere speciale.

- **Unicità e Imprevedibilità** – L'utente evita l'uso di informazioni personali facilmente accessibili o indovinabili, come date di nascita o nomi (compresi nomi di account predefiniti o facilmente riconoscibili, come da es. utente, user, ecc…).
- **Gestione Sicura delle Password –** L'utente implementa pratiche sicure di gestione delle password; evita di visualizzare le password durante la digitazione; cambia la password al 1° accesso; inoltre il sistema informativo di Ateneo impone il cambio password almeno ogni 150 giorni, non consentendo di impostare password utilizzate in precedenza.
- **Sicurezza dell'Accesso** – Il Sistema informativo blocca per un periodo definito di tempo l'account dopo un determinato numero di tentativi di accesso falliti. Le credenziali devono essere convalidate solo dopo l'inserimento completo e corretto di tutti i dati, e la sessione di accesso (di seguito anche login) deve essere terminata se non completata entro un tempo stabilito.
- **Dopo il Login** - Ove possibile, l'Ateneo fornisce all'utente informazioni utili dopo il login, come la data e l'ora dell'ultimo accesso riuscito e dettagli sui tentativi falliti successivi, al fine di consentire all'utente di analizzare eventuali accessi non autorizzati al proprio account; da comunicare tempestivamente alla struttura deputata al coordinamento della sicurezza informatica ed alla struttura ICT della propria sede (v. Regolamento art. 3).
- **Protezione delle Password** – L'Ateneo utilizza la crittografia (hash salted) per la memorizzazione sicura delle password; l'utente è invitato a non memorizzare le credenziali di accesso nel browser; a tale fine possono essere implementate politiche di sicurezza per prevenire tale azione.
- **Monitoraggio e Audit** – Il Sistema Informativo traccia sia gli accessi riusciti che i tentativi falliti; esegue audit regolari per identificare possibili attacchi.
- **Controllo dell'IP Sorgente** - Il Sistema Informativo valida l'indirizzo di rete IP (Internet Protocol) per applicazioni intranet o internet, con particolare attenzione agli accessi da IP esterni o sospetti.
- **Aggiornamento e Riesame dei Requisiti** – L'Ateneo rivedere periodicamente i requisiti di sicurezza per mantenere o aumentare la protezione delle password in linea con le minacce emergenti.

Queste misure mirano a rafforzare la sicurezza delle password attraverso la combinazione di buone pratiche di creazione, gestione e protezione delle credenziali, riducendo così il rischio di accessi non autorizzati e compromissioni.

4. Specifiche generali per il mantenimento in attività delle utenze

Per minimizzare i rischi di compromissione dei sistemi informativi e adottare prassi di contenimento dei costi di gestione correlati, l'Ateneo adotta politiche di periodica valutazione dello spazio disco (cloud), risorse di calcolo e banda di trasmissione di dati resi disponibili agli utenti, anche in relazione agli standard di riferimento dei servizi cloud correlati, tenendo conto dell'oscillazione delle dinamiche di prezzo, a fronte del monitoraggio dell'andamento dei vari contratti di servizio in essere.

Politica per la gestione degli incidenti di sicurezza informatica

In fase di prima approvazione del regolamento per tale politica si fa riferimento alla prassi definita alla pagina https://www.uniupo.it/it/ateneo/regolamenti-trasparenza-sindacati/protezione-dei-dati-personali, con particolare riferimento alle funzioni dell'Incident Response Team. Cfr.:

- D.R. rep. n. 390/2019 del 19.03.2019;
- D.R. Rep. n. 1633/2022, prot. n. 142262 del 17.10.2022.