Università di Genova

Emanato con D.R. n. 2847 del 3.07.2026

Pubblicato in albo informatico di Ateneo il 6.07.2026 – in vigore dal 3.07.2026

A cura dell'Area ICT

# REGOLAMENTO DI ATENEO PER LA SICUREZZA INFORMATICA

Previsto ai sensi del D.lgs. 4 settembre 2024 n. 138 (recepimento Direttiva NIS2)

Sommario



Approvato con delibera del Consiglio di Amministrazione n. 165 del 30 giugno 2026.

## Art. 1 - Finalità e ambito di applicazione

1. L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe"), in qualità di soggetto importante ai fini dell'attuazione della Direttiva UE 2022/2555 (NIS2) sulla cybersicurezza (di seguito anche "Direttiva"), come recepita col D.lgs. n. 138/2024 (di seguito "Decreto NIS2"), adotta il presente regolamento quale strumento di sviluppo, governo, gestione, monitoraggio e miglioramento della sicurezza informatica di Ateneo. Il regolamento integra le disposizioni vigenti in materia di protezione dei dati personali, amministrazione digitale e sicurezza ICT, come previsto dalla normativa vigente in materia e dalle determine dell'Agenzia per la Cybersicurezza Nazionale (di seguito ACN), dall'Agenzia Nazionale per l'Italia Digitale (AGID), in coerenza con lo Statuto e i regolamenti di Ateneo.

2. Il regolamento disciplina l'organizzazione e le responsabilità per garantire un livello elevato di cybersicurezza, in coerenza con i principi di gestione del rischio e di protezione dei dati anche personali, sin dalla progettazione del sistema informativo e dei servizi. Le misure tecniche e i modelli architetturali specifici sono definiti e aggiornati in appositi allegati, al fine di garantire il costante adeguamento all'evoluzione tecnologica e alle minacce informatiche.

3. Gli obiettivi inerenti alla cybersicurezza sono integrati nell'ambito dei documenti programmatori di Ateneo, quali, ad esempio, il Piano Integrato di Attività e Organizzazione (PIAO).

4. L'Organizzazione e le prassi connesse alla cybersicurezza sono anche concepite per facilitare l'esercizio dei diritti degli interessati in tema di privacy (es. il diritto di accesso, rettifica, cancellazione dei dati personali), garantendo che i dati siano rintracciabili, correggibili e cancellabili in conformità alle richieste legittime.

## TITOLO I – GOVERNANCE E RESPONSABILITA'

1. Il presente Titolo soddisfa il seguente requisito obbligatorio previsto dalle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 1 | Organizzazione per la sicurezza informatica | GV.RR-02 p. 1 |

## Art. 2 - Struttura organizzativa del sistema di sicurezza informatica di Ateneo

1. La governance e il modello di responsabilità inerenti alla cybersicurezza di UniGe sono applicati conformemente al modello organizzativo dell'Ateneo. Il modello organizzativo e delle responsabilità della cybersicurezza comprende le seguenti figure:

a) Organi di amministrazione e direttivi NIS2 (d'ora in poi anche "Organi"): Rettore; componenti del Consiglio di Amministrazione, Direttore generale;
b) Commissione per la cybersicurezza;
c) Responsabile per la Transizione Digitale (RTD) ai sensi dell'art. 17 del D.lgs. 82/2005 e s.m.i., ed Area competente per i sistemi informativi di Ateneo (di seguito, Area ICT);
d) Dirigenti e soggetti assimilati ai dirigenti ai fini del presente regolamento: presidi di scuola; direttori di dipartimento; presidenti dei centri di servizi di Ateneo; direttori dei centri interuniversitari di ricerca e di servizio; direttori dei centri di eccellenza; presidente di IANUA; responsabili scientifici delle attività di didattica e ricerca e dei laboratori;
e) Punto di Contatto NIS2 e sostituto del punto di contatto NIS2;
f) Incident Response Team e Referenti CSIRT;
g) DPO, Responsabile della protezione dati;
h) Amministratori di Sistema (AdS);

i) Personale docente e tecnico amministrativo, bibliotecario, sociosanitario (d'ora in poi, personale TABS), collaboratori ed esperti linguistici (CEL) e altri lavoratori subordinati;
j) Altro personale che collabora a qualsiasi titolo con l'Ateneo (docenti a contratto, assegnisti, borsisti, visiting professors e visiting researchers, cultori della materia, ecc…) e studenti.

2. I ruoli e le responsabilità di cui al punto 1 sono riesaminati e, se opportuno, aggiornati periodicamente almeno ogni due anni, nonché qualora si verifichino incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

## Art. 3 - Organi di Amministrazione e direttivi NIS2

1. Gli Organi di cui all'art. 2 comma 1, lett. a), secondo il Decreto NIS2 e in base alle rispettive competenze statutarie:

a) sovrintendono all'attuazione delle misure di sicurezza informatica;
b) sovrintendono all'assolvimento degli obblighi formativi in tema di cybersicurezza nei confronti dei dipendenti dell'Ateneo;
c) approvano il presente regolamento, le politiche di sicurezza, i piani previsti in base alle disposizioni normative e regolatorie, verificando periodicamente l'efficacia delle misure adottate, ai sensi dell'art. 23 del Decreto NIS2;
d) assicurano che la gestione del rischio per la sicurezza dei sistemi informativi e di rete sia integrata nei processi decisionali strategici, organizzativi e finanziari dell'Ente, anche in coerenza con il ciclo della performance;
e) si mantengono costantemente aggiornati rispetto al contesto della cybersicurezza, attraverso iniziative di informazione e formazione. Tale formazione è da ritenersi obbligatoria per tali Organi e per tutti gli altri soggetti di cui all'art 2 comma 1, secondo le modalità definite nel Piano di formazione di cui all'art. 22;
f) garantiscono l'assegnazione di risorse umane, tecnologiche e finanziarie adeguate all'attuazione delle misure di sicurezza, alla gestione degli incidenti e alla continuità operativa dei servizi istituzionali;
g) esercitano tutte le ulteriori funzioni di monitoraggio, controllo, ed indirizzo strategico, in base a quanto previsto dalla norma e delle loro specifiche competenze statutarie.

2. Gli atti di cui al comma 1, lett. c) sono predisposti dal Responsabile per la Transizione Digitale (RTD), attraverso il suo ufficio di supporto, con la fattiva collaborazione dei dirigenti e dei soggetti di cui all'art. 2 comma 1, lett. d), ciascuno per quanto di competenza.

3. Le forme di collaborazione di cui al precedente comma, nonché le modalità di coinvolgimento e partecipazione di altre figure competenti sono definite dal Responsabile per la transizione digitale, sentito il Direttore generale. I soggetti di cui all'art. 2 comma 1, lett. d), assicurano la collaborazione del personale che da essi dipende funzionalmente o gerarchicamente.

## Art. 4 - Commissione per la Cybersicurezza

1. La Commissione per la Cybersicurezza ha funzioni propositive e consultive rispetto alla governance della Cybersicurezza di Ateneo. Definisce le priorità e individua le migliori prassi organizzative, tecnologiche e regolamentari ai fini della pianificazione, progettazione, gestione, monitoraggio e riesame della sicurezza informatica di Ateneo, supportando gli Organi nelle opportune decisioni e deliberazioni, anche connesse agli adempimenti previsti a livello comunitario e nazionale.

## Art. 5 - Responsabile per la Transizione Digitale (RTD) e Area ICT

1. Il Responsabile per la Transizione Digitale (RTD), ai sensi del Codice dell'Amministrazione Digitale (D.lgs. 82/2005 e s.m.i.):

a. coordina le attività inerenti allo sviluppo e alla gestione dei sistemi informativi di Ateneo nonché alla sicurezza dei sistemi informativi e di rete, in raccordo con l'Area dirigenziale competente per i sistemi informativi (di seguito anche Area ICT), sulla base degli indirizzi degli Organi;

b. elabora i documenti di cui all'art. 3 comma 1, lett. c) e i relativi aggiornamenti;

2. L'Area ICT assicura il coordinamento dell'attuazione delle politiche di sicurezza, la gestione tecnica delle infrastrutture ICT ad essa affidate, il monitoraggio degli eventi di cybersicurezza, il supporto ICT alle strutture didattiche, di ricerca e amministrative, il raccordo funzionale tra le politiche di cybersicurezza definite dagli Organi di governo verso le suddette strutture.

3. L'Area ICT collabora con il Punto di Contatto NIS2, con l'Incident Response Team e con i Referenti CSIRT, di cui all'art. 8, ai fini della gestione e notifica degli incidenti, nonché dell'attuazione delle eventuali misure correttive richieste dalle Autorità competente.

## Art. 6 - Dirigenti e soggetti assimilati ai dirigenti

1. I dirigenti e i soggetti di cui all'art. 2, comma 1, lett. d) nell'ambito delle rispettive competenze, come stabilite dallo Statuto, dai regolamenti e dagli altri atti di organizzazione, sono responsabili dell'adempimento degli obblighi in materia di:

a) collaborazione alla predisposizione e aggiornamento delle politiche e dei piani di cui all'art. 3 comma 1, lett. c);

b) attuazione delle politiche e dei piani di cui all'art. 3, comma 1, lett. c), nonché collaborazione alla verifica periodica dell'efficacia delle misure adottate;

c) coordinamento del supporto alla notifica degli incidenti significativi ai sensi dell'art. 25 del Decreto NIS2, rispetto alla struttura di afferenza;

d) attuazione delle prescrizioni e raccomandazioni eventualmente impartite dall'Autorità nazionale competente NIS, dagli Organi di Ateneo e dal RTD;

e) verifica delle competenze professionali in ambito di cybersicurezza e dello sviluppo delle stesse nell'ambito della propria struttura;

f) validazione, in caso di Direttori di Struttura / dirigenti del censimento degli asset rientranti nel perimetro della cybersicurezza, come da art 13, comma 4 lett. a;

2. Ai dirigenti e ai soggetti di cui all'art. 2, comma 1, lett. d) sono fornite la formazione specifica e il supporto ai fini dell'assolvimenti dei propri compiti.

## Art. 7 - Responsabili scientifici delle attività di didattica o di ricerca o dei laboratori

2. Qualora esigenze scientifiche o didattiche, adeguatamente motivate, richiedano configurazioni o specifiche tecniche non standard rispetto alle politiche di cybersicurezza generali, esse devono essere preventivamente richieste dall'interessata/o e dal direttore della struttura cui lo stesso afferisce all'Area ICT, secondo i criteri previsti all'art 13 e in coerenza con le disposizioni previste dalla *Politica di classificazione degli asset informatici* di cui all'allegato 1 nonché dalla *Politica per la sicurezza dell'infrastruttura informatica* di cui all'allegato 2.

3. I responsabili di cui al presente articolo cooperano attivamente e in modo costante alla classificazione degli asset, alla valutazione del rischio e all'adozione delle misure di protezione adeguate, in coerenza con la mappatura dei livelli di rischio correlati ai dati gestiti di cui al all'allegato 1, con specifico riferimento ai casi di trattamento di dati particolari, dati di ricerca strategici o infrastrutture tecnologiche rilevanti ai fini della continuità operativa delle attività istituzionali dell'Ateneo.

## Art. 8 - Punto di Contatto NIS2 e suo sostituto - Incident Response Team e Referenti CSIRT

1. Ai sensi dell'art. 7 comma 1 del Decreto NIS2 e s.m.i., e delle determinazioni adottate dall'Agenzia per la Cybersicurezza Nazionale in materia, il Rettore designa tra il personale docente, o dirigente, o TABS un soggetto cui attribuire le funzioni di Punto di Contatto NIS2, nonché uno o più sostituti.

2. Il Punto di Contatto NIS2, o Sostituto:

a) cura gli adempimenti di registrazione e aggiornamento delle informazioni sulla piattaforma digitale ACN;

b) rappresenta l'Ateneo nelle interlocuzioni con l'Autorità nazionale competente NIS2;

c) coordina, per quanto di competenza, la gestione delle notifiche di incidente significativo.

3. Il Rettore, su proposta del Punto di Contatto NIS2, designa:

a. i componenti dell'Incident Response Team, ossia un gruppo di persone incaricate della gestione e mitigazione degli incidenti informatici di Ateneo ai sensi dell'art. 25 del Decreto NIS2;

b. i referenti CSIRT, ossia soggetti incaricati di interloquire operativamente con il CSIRT Italia e con altre autorità di settore, anche al fine di effettuare le notifiche di incidente nei termini previsti dalla normativa vigente, in base alle direttive impartite dall'Incident Response Team.

4. Il Punto di Contatto NIS2 / Sostituto/i, i componenti dell'Incident Response Team e i referenti CSIRT devono possedere adeguate competenze in materia di ICT e di sicurezza informatica, nonché conoscenza dell'assetto organizzativo e tecnologico dell'Ateneo.

5. Le funzioni dell'Incident Response Team e dei referenti CSIRT sono contenute nella normativa vigente nonché nelle delibere del Consiglio di amministrazione per quanto attiene alla procedura di gestione degli incidenti.

## Art. 9 - DPO, Responsabile della protezione dati

1. Il DPO è consultato dai soggetti di cui al Titolo I, ciascuno secondo le proprie attribuzioni, ai fini della redazione e aggiornamento del Regolamento e delle policy, della gestione del rischio, della gestione di incidenti informatici (ed eventuali data breach, ove relativi a dati personali).

## Art. 10 - Amministratori di Sistema

1. Gli Amministratori di Sistema (di seguito AdS) sono individuati in coerenza con le disposizioni del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i., del Decreto NIS2 e s.m.i, e delle Determinazioni dell'Agenzia ACN, a cura dei referenti al trattamento dati, come previsti dal *Regolamento dell'Università degli studi di Genova in materia di trattamento dei dati personali*, in coerenza con Linee guida Amministratori di Sistema, approvate dal Consiglio di amministrazione.

2. Gli AdS operano nel rispetto dei principi di minimo privilegio, separazione delle funzioni, tracciabilità delle operazioni, protezione delle credenziali privilegiate, assicurando la continuità del processo di censimento e caratterizzazione degli *asset* ICT gestiti al fine di consentire la valutazione del rischio *cyber* correlato.

3. Le attività svolte dagli amministratori di sistema sono oggetto di tracciamento e registrazione mediante opportuni sistemi, in conformità alla normativa.

4. L'Ateneo assicura la distinzione tra utenze ordinarie e utenze con privilegi amministrativi elevati, come previsto dalla *Politica per la Sicurezza degli asset informatici*, di cui all'allegato 2, ove tecnicamente possibile, nonché la verifica periodica della permanenza dei requisiti di autorizzazione.

5. Le Linee Guida Amministratori di Sistema definiscono il processo di individuazione e gestione dell'archivio degli amministratori di sistema, le loro funzioni dettagliate e la loro interazione rispetto alla Direttiva NIS2.

## Art. 11 - Personale dipendente dell'Ateneo

1. Il personale dipendente di Ateneo:

a) partecipa alla formazione obbligatoria sulla cybersicurezza, organizzata dall'Ateneo;

b) adotta le misure per il contenimento dei rischi cyber, in coerenza con il piano di gestione del rischio cyber, e con le circolari applicative e/o linee guida che a tal fine possono essere emanate dal Direttore Generale, anche su proposta del Responsabile della Transizione Digitale;

c) coopera attivamente con l'Incident Response Team, segnalando il rischio del verificarsi di un incidente informatico, ovvero il verificarsi di un incidente, sulla base Linee guida per la gestione degli incidenti, di cui all'art. 20;

d) partecipa alla classificazione degli asset della struttura, in coerenza con il ~~r~~uolo rivestito.

## Art. 12 - Altro personale e Studenti

1. Gli studenti e i soggetti di cui all'art. 2, comma 1, lett. j) si attengono alle disposizioni del presente regolamento, alle politiche in materia di *cybersicurezza* di Ateneo nonché alle istruzioni impartite da UniGe anche mediante campagne informative e di sensibilizzazione sulla materia.

# TITOLO II – GESTIONE DELLA SICUREZZA INFORMATICA

## Art. 13 - Gestione del rischio per la sicurezza informatica

1. L'Ateneo adotta e mantiene aggiornati i seguenti Piani, come previsti delle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 3 | Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete | ID.RA-05 p. 3 |
| 4 | Piano di trattamento del rischio | ID.RA-06 p. 3 |
| 6 | Piano di adeguamento | ID.IM-01 p. 1 |

2. Detti piani sono riesaminati almeno ogni due anni, o in occasione di incidenti significativi o di mutamenti organizzativi, e approvati dal Consiglio di amministrazione, previo parere del Senato accademico, per i casi previsti.

3. I Piani di cui al comma 1 sono articolati nelle fasi prescritte dal Common Security Framework 2.0 e s.m.i., ossia GOVERN, IDENTIFY, PROTECT e si fondano sull'identificazione,

la misurazione e la valutazione del rischio, sulla definizione di misure, anche coordinate fra loro, di prevenzione, trattamento e gestione del rischio medesimo, con la definizione di priorità, responsabilità e tempistiche di attuazione, secondo criteri di adeguatezza organizzativa, gradualità, ragionevolezza e proporzionalità.

4. I Piani di cui al comma 1 definiscono le seguenti attività propedeutiche minime, che devono prevedere i corretti schemi di aggiornamento e manutenzione dei dati, a cura della Area ICT, degli Amministratori di sistema (AdS), di cui all'art. 10, e dei Responsabili scientifici delle attività di didattica o di ricerca o dei laboratori, di cui all'art. 7, secondo le rispettive competenze previste al Titolo I:

a) censimento e caratterizzazione costante degli *asset* anche finalizzato alla loro classificazione in base al livello di criticità dei dati gestiti, validato dal responsabile di struttura, come da art. 6 comma 1 lett. f.;

b) definizione di una procedura che, sulla base di raggruppamenti omogenei di *asset*, definisca il relativo livello di rischio in termini di probabilità ed impatto (*magnitudo*) sulla continuità delle attività, anche attraverso l'utilizzo di sistemi di raccolta delle informazioni integrati e centralizzati;

c) individuazione delle misure correttive e/o di contenimento del rischio *cyber* anche intese in termini di definizione di un campione definito di casi d'uso, che coprano le principali casistiche di protezione e mitigazione dei rischi, e che comprendano anche le interazioni con altri enti pubblici e privati e con i fornitori, in ottica di sicurezza della *supply chain* ICT;

d) implementazione delle misure correttive e/o di contenimento del rischio, di tipo tecnico organizzativo. In caso di valutazioni che comportino l'applicazione di casi d'uso già definiti in sede di valutazione del rischio, ovvero prassi documentate, l'implementazione delle misure correttive è di competenza diretta degli Amministratori di Sistema (Ads) e dei Responsabili scientifici delle attività di didattica – ricerca o dei laboratori;

e) *audit* e monitoraggio al fine di supportare il miglioramento costante del processo.

L'attività di cui al presente articolo è svolta in coerenza con le corrispondenti procedure previste dal GDPR, ed in particolare con la prassi della Data Protection Impact Analysis (DPIA), ove prevista.

5. La gestione del rischio si applica a tutte le strutture di Ateneo, inclusi i contesti di ricerca e sviluppo. In questi ultimi, ove l'attuazione delle misure tecniche riportate nel seguito e negli Allegati non sia pienamente applicabile per vincoli tecnici ovvero operativi, la messa in sicurezza dell'ambiente è definito d'intesa con l'Area ICT, previa analisi di impatto del cyber rischio, individuando misure compensative concordate e proporzionate al livello di rischio, nel rispetto delle competenze attribuite ai soggetti di cui al Titolo I.

6. In prima applicazione, nelle more del completamento dell'analisi del rischio a livello delle diverse strutture e della definizione delle misure di trattamento del rischio, in relazione agli asset di ricerca e sviluppo l'analisi del rischio comprende almeno: i) le caratteristiche dell'asset, secondo lo schema di censimento dell'asset approvato dal Consiglio di Amministrazione, comprendente la descrizione della sue finalità; ii) l'analisi di eventuali vulnerabilità e rischi; iii) il trattamento del rischio.

## Art. 14 - Sicurezza dell'infrastruttura informatica, di rete e dei dati

1. L'Ateneo adotta e mantiene aggiornato il seguente Piano, come previsto dalle disposizioni NIS2. Esso si identifica con gli allegati indicati nel presente articolo, nonché le Politiche della sicurezza fisica di cui al successivo art. 15.

| # | Documento | Requisito |
|---|---|---|
| 2 | Politiche di sicurezza informatica | GV.PO-01 p. 1 |

2. L'Ateneo definisce livelli generali di classificazione degli asset del proprio sistema informativo mediante una specifica politica denominata **Politica di Classificazione degli Asset informatici di cui all'Allegato 1**. Per asset si intendono, a titolo esemplificativo e non esaustivo, reti, sistemi, dispositivi, identità digitali, attività e servizi digitali, applicazioni, archivi di dati strutturati o non strutturati.

3. La Politica, di cui all'allegato 1, definisce le diverse tipologie di asset individuando le relative modalità di classificazione utili alla gestione degli stessi nonché gli approcci generali e minimi volti alla loro protezione. Detta classificazione è un processo dinamico che:

a) è coerente con le differenti attività caratterizzanti la missione istituzionale dell'Ateneo (didattica, ricerca, terza missione, amministrazione) nonché con gli strumenti tecnici adottati;

b) si adatta ad attività di produzione nonché di ricerca e sviluppo e, costantemente, all'evoluzione tecnologica, al mutamento dei livelli di rischio degli asset stessi nonché al livello di riservatezza e criticità dei dati gestiti in essi;

4. Una volta stabilite le modalità di classificazione di cui al comma 2, sono definite le conseguenti regole di protezione, che sono elencate nella **Politica per la Sicurezza degli asset informatici, di cui all'Allegato 2.** Dette regole sono aggiornate e precisate in base all'evoluzione tecnologica, all'esperienza, e agli audit, e sono basate sui seguenti principali principi chiave:

a) minima esposizione,

b) difesa in profondità,

c) segregazione delle reti,

d) protezione del dato,

e) governo delle identità,

f) controllo degli accessi,

g) ciclo di vita sicuro del software,

h) ulteriori soluzioni previste dalla normativa europea e nazionale anche guidati da proporzionalità e valutazione del rischio.

5. Le politiche di protezione di cui agli allegati 1 e 2 sono coerenti con il Regolamento UE 2016 679 (GDPR) e col *Regolamento per il trattamento dei dati personali*.

## Art. 15 - Sicurezza fisica a protezione degli asset ICT

1. Il presente regolamento definisce la **Politica della sicurezza fisica, di cui all'allegato 3**, nel rispetto delle disposizioni per la sicurezza fisica dei locali contenenti archivi informatici, ai sensi della normativa vigente in materia di protezione dei dati personali.

## Art. 16 - Continuità operativa

1. L'Ateneo adotta e mantiene aggiornati i seguenti Piani, come previsti delle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 7 | Piano di continuità operativa | ID.IM-04 p. 1 |
| 8 | Piano di ripristino in caso di disastro | ID.IM-04 p. 1 |

2. Detti piani sono riesaminati almeno ogni due anni e approvati dal Consiglio di amministrazione, previo parere del Senato accademico, per i casi previsti.

3. L'Ateneo effettua tipicamente su base annuale test di continuità operativa (Business Continuity) dei servizi, cui sia attribuito un livello di cyber rischio elevato.

## Art. 17 - Gestione identità digitale, autenticazione, autorizzazione e controllo accessi

1. L'accesso ai sistemi informativi e di rete è orientato secondo i principi del minimo privilegio e della separazione dei ruoli e delle funzioni. L'implementazione conseguente si avvale dei principali paradigmi di sicurezza aggiornati allo stato dell'arte, in coerenza con le disponibilità tecniche, organizzative ed economiche dell'Ateneo.

2. Sono considerati fondamentali i seguenti paradigmi o tecnologie, da aggiornare anche in base all'evoluzione tecnologica in relazione ai sistemi di produzione:

a) riconducibilità certa dell'identità digitale;

b) governo degli accessi;

c) responsabilità ed uso corretto dell'identità digitale;

d) monitoraggio e tracciabilità.

3. Per gli ambienti di ricerca e sviluppo presenti nei Dipartimenti / Centri di ricerca, si applicano le misure previste all'art. 13.

## Art. 18 - Gestione dei log

1. L'accesso ai contenuti dei *log* è soggetto a rigorose limitazioni ed è consentito esclusivamente per finalità connesse al corretto funzionamento dei sistemi informativi, alla sicurezza, al monitoraggio, alla gestione degli incidenti, all'audit e agli adempimenti normativi, nel rispetto delle disposizioni previste nello Statuto dei lavoratori e dalla normativa in materia di trattamento dei dati personali.

2. L'accesso ai log deve avvenire esclusivamente da parte di soggetti autorizzati, previamente individuati in relazione alle rispettive funzioni e competenze, sulla base del principio di necessità e minimizzazione, per finalità documentate e verificabili. Gli accessi ai log devono essere tracciati e sottoposti a misure di controllo idonee a prevenire accessi non autorizzati, utilizzi impropri o trattamenti illeciti dei dati.

3. La gestione dei log è svolta dall'Area ICT, dagli Amministratori di sistema, dai Responsabili scientifici delle attività di didattica, di ricerca o dei laboratori per quanto di competenza, ovvero da altri soggetti delegati ed opportunamente nominati come responsabili del trattamento dei dati ai sensi dell'art. 28 GDPR, a fronte della verifica del possesso di idonei requisiti di competenza professionale posseduta dagli stessi.

4. I log devono essere conservati e mantenuti secondo criteri di adeguatezza, integrità e sicurezza, per un periodo di tempo necessario e conforme alle disposizioni di legge applicabili e di Ateneo, in coerenza con le prassi di scarto e con le policy di conservazione documentale adottate dall'Ateneo.

5. L'Ateneo adotta inoltre idonee misure tecniche e organizzative per prevenire la perdita dei dati dei log, la loro alterazione o l'accesso da parte di soggetti non autorizzati.

6. La gestione dei log, ove tecnicamente possibile, avviene in modalità centralizzata.

## Art. 19 - Gestione delle vulnerabilità

1. L'Ateneo adotta e mantiene aggiornato il seguente Piano, come previsto dalle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 5 | Piano di gestione delle vulnerabilità | ID.RA-08 p. 4 |

1. Il processo di gestione delle vulnerabilità si articola nelle seguenti fasi:

a) raccolta delle vulnerabilità: l'organizzazione raccoglie informazioni sulle vulnerabilità da fonti qualificate;

b) prima valutazione e prioritizzazione analisi delle vulnerabilità: è assegnata una prima priorità in base al rischio associato e al costo della bonifica, con coinvolgimento iniziale dell'Amministratore di sistema (referente tecnico locale della struttura) e/o del Responsabile scientifico delle attività di didattica e ricerca / laboratorio;

c) valutazione e prioritizzazione: le vulnerabilità ritenute rilevanti sono valutate e prioritizzate dall'Incident Response team, considerando: gravità tecnica, esposizione degli asset, criticità dei sistemi coinvolti, contesto operativo e disponibilità di misure compensative. Tale procedura consente di stabilire, in funzione del processo di gestione del rischio, le misure da adottare per accettare, mitigare o eliminare il rischio medesimo. La responsabilità della valutazione finale è attribuita all'Area ICT e comunicata all'Amministratore di sistema e/o al Responsabile scientifico delle attività di didattica e ricerca / laboratorio e/o ai fornitori ed erogatori dei servizi IT per l'assunzione delle opportune azioni. Il **Piano di gestione delle vulnerabilità** definisce nel dettaglio le relative procedure;

d) risoluzione (patching o mitigazione): l'Amministratore di sistema e/o il responsabile scientifico delle attività di didattica e ricerca / laboratorio e/o i fornitori o erogatori dei servizi IT procedono all'applicazione di misure patch di sicurezza o all'implementazione di soluzioni temporanee (workaround) o definitive per sanare le falle. A seguito dell'analisi del rischio e dell'individuazione delle misure compensative sono definite soluzioni strutturali;

e) rivalutazione: sui sistemi che hanno presentato vulnerabilità sono eseguite periodicamente nuove scansioni per verificare l'efficacia delle azioni correttive.

2. In caso di inosservanza delle indicazioni ricevute in ordine alla mitigazione delle vulnerabilità, ovvero in caso di necessità di intervento correlata a rischi significativi, l'Area ICT adotta misure compensative proporzionate, quali, a titolo esemplificativo:

a) limitazione dell'accesso di rete;

b) segmentazione o isolamento del sistema;

c) rafforzamento dei controlli di autenticazione;

d) disabilitazione di servizi o componenti non essenziali.

3. L'adozione di tali misure deve essere tempestivamente notificata al personale eventualmente interessato e al responsabile della struttura, specificandone le motivazioni tecniche, secondo le disposizioni normative, e le linee guida previste dalle autorità regolatorie.

## Art. 20 - Gestione e notifica degli incidenti

1. L'Ateneo adotta e mantiene aggiornato il seguente Piano, come previsto dalle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 11 | Piano per la gestione degli incidenti di sicurezza informatica | RS.MA-01 p. 2 |

2. Gli incidenti di sicurezza sono gestiti secondo una procedura formalizzata che distingue tra incidente ordinario e incidente significativo ai sensi del Decreto NIS2.

3. In caso di rischio o al verificarsi di un incidente di cui al comma 1, l'Amministratore di Sistema e/o il Responsabile scientifico delle attività di didattica – ricerca o dei laboratori adottano azioni proattive, con il massimo delle tempestività, per coordinarsi con l'Incident Response Team, secondo la **Procedura di gestione degli incidenti di cui all'Allegato 4**, approvate dal Consiglio di amministrazione.

## Art. 21 - Gestione delle crisi

1. L'Ateneo adotta e mantiene aggiornato il seguente Piano, come previsto dalle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 9 | Piano di gestione delle crisi | ID.IM-04 p. 1 |

2. Per crisi informatica si intende qualsiasi evento derivante da incidenti ICT, di natura dolosa o accidentale, che comprometta in modo significativo la disponibilità, l'integrità o la riservatezza dei sistemi informativi, dei dati o dei servizi ICT essenziali dell'Ateneo.

3. Al verificarsi di un evento qualificabile come crisi, l'Ateneo procede alla relativa dichiarazione formale alle autorità competenti, ai sensi dell'art. 20, per mezzo di un referente CSIRT, attivando tempestivamente i canali di comunicazione interna ed esterna, nel rispetto degli obblighi normativi vigenti e dalle disposizioni nazionali in materia di cybersicurezza. La comunicazione è assicurata nei confronti degli Organi dell'Ateneo, delle strutture interessate e, ove necessario, degli utenti e dei soggetti terzi coinvolti.

4. Nel corso della gestione della crisi, l'Ateneo opera in base agli indirizzi degli organismi governativi competenti, inclusa l'ACN, lo CSIRT Italia e le altre autorità eventualmente coinvolte, conformandosi alle loro disposizioni, raccomandazioni e misure operative da questi impartite.

5. Contestualmente alla dichiarazione di crisi, è attivato un protocollo interno di continuità operativa minimale, volto a garantire il mantenimento o il rapido ripristino delle funzioni essenziali dell'Ateneo, attraverso misure temporanee e prioritarie di gestione dei servizi critici, anche in condizioni degradate o emergenziali.

6. La gestione della crisi coinvolge tutti gli attori rilevanti, interni ed esterni all'Ateneo, inclusi i fornitori di servizi ICT, i partner tecnologici e i soggetti pubblici o privati interessati, i quali sono tenuti a cooperare attivamente secondo quanto previsto dai contratti e dalle disposizioni applicabili, al fine di assicurare il contenimento dell'incidente, il ripristino delle condizioni di sicurezza e la mitigazione degli impatti.

## Art. 22 - Formazione e sviluppo della consapevolezza in materia di cybersicurezza

1. L'Ateneo adotta e mantiene aggiornato il seguente Piano, come previsto dalle disposizioni NIS2.

| # | Documento | Requisito |
|---|---|---|
| 11 | Piano di formazione | PR.AT-01 p. 1 |

2. Il Piano di cui al comma 1 ricomprende i soggetti di cui al Titolo I, con priorità rispetto alle figure che rivestono funzioni di responsabilità di governo, di direzione, di amministrazione di sistemi informativi.

3. Tale Piano è altresì finalizzato ad assicurare un adeguato livello di competenze, consapevolezza e responsabilizzazione del personale rispetto ai rischi cyber e alle misure di sicurezza adottate.

4. La formazione in materia di cybersicurezza prevista dal Piano di cui al comma 1 è integrata con il PIAO.

5. L'Ateneo traccia le attività formative svolte in materia di cybersicurezza e adotta un sistema di rilevazione della qualità della formazione coerente con il relativo sistema di Ateneo.

6. L'Ateneo adotta iniziative specifiche rivolte agli studenti e alla propria comunità, con l'obiettivo di promuovere una più ampia cultura della cybersicurezza, accrescere il livello di consapevolezza ed attenzione rispetto ai rischi informatici e favorire comportamenti consapevoli e responsabili nell'utilizzo delle tecnologie digitali.

7. Le rappresentanze studentesche assicurano un'attività proattiva di informazione e comunicazione, nonché di sensibilizzazione di tutta la comunità studentesca sui temi della cybersicurezza.

# TITOLO III - SICUREZZA CATENA DI APPROVVIGIONAMENTO ICT (SUPPLY CHAIN ICT)

## Art. 23 - Principi generali in materia di sicurezza della supply chain ICT

1. L'Ateneo adotta un approccio sistemico relativo alla sicurezza della catena di approvvigionamento ICT (supply chain ICT), quale elemento essenziale per la tutela delle proprie funzioni istituzionali e della sicurezza dei dati trattati. A tale fine coopera con l'Agenzia ACN, ovvero altri soggetti aventi funzione regolatoria, al censimento dei fornitori ICT ritenuti rilevanti ai sensi del Decreto NIS2 e s.m.i., con particolare riferimento alle attività e servizi ICT indicate nell'Allegato I del medesimo decreto, nonché sulla base delle determine dell'Agenzia stessa.

## Art. 24 - Requisiti di sicurezza dei fornitori

1. L'Ateneo richiede ai fornitori il rispetto di requisiti minimi di sicurezza, con particolare riferimento all'adozione di misure tecniche e organizzative idonee a garantire riservatezza, integrità e disponibilità dei dati, anche in coerenza con standard quali ISO/IEC 27001, ed in particolare secondo un processo che consenta di ricostruire la tracciabilità della procedura e dei componenti che costituiscono la fornitura o il servizio.

2. Gli operatori economici sono in ogni caso responsabili della conformità dei loro beni e servizi alle normative vigenti e ne danno atto nelle partecipazioni alle gare e nei documenti contrattuali, anche per quanto riguarda la conformità dei loro fornitori, subappaltatori e subcontraenti.

3. Il fornitore è designato responsabile del trattamento ai sensi dell'art. 28 GDPR e del regolamento di Ateneo in materia, quando tratta dati personali per conto dell'Ateneo.

4. È inoltre promossa la trasparenza della supply chain tecnologica, anche attraverso informazioni sui componenti utilizzati secondo logiche assimilabili al Bill of Materials o Software Bill of Materials, con particolare riferimento alle procedure di gara, di cui all'art. 27.

5. Nel caso di forniture realizzate in house per mezzo di software libero "Open source", ovvero acquisire con il concorso di terzi, le stesse si conformano ai medesimi principi di sicurezza e tracciabilità di cui al presente Titolo.

## Art. 25 - Albo dei fornitori e supply chain

1. L'Ateneo si può dotare di un proprio albo ovvero aderire ad albi costituiti con altri soggetti pubblici / privati per l'individuazione dei fornitori ICT accreditati, quale strumento di supporto alla gestione del rischio della supply chain.

2. È prevista l'individuazione di criteri di controllo periodico, anche a campione, dell'adeguatezza delle procedure e dei contratti di acquisto di beni e servizi ICT rispetto alle disposizioni previste.

## Art. 26 - Disposizioni particolari per attività di ricerca e sperimentazione

1. Per esigenze connesse alle attività di ricerca e sperimentazione, possono essere ammesse deroghe motivate ai requisiti di sicurezza, qualora non siano disponibili soluzioni alternative conformi. In tali casi si applicano i criteri di analisi e valutazione del rischio di cui all'art. 13.

## Art. 27 – Criteri di sicurezza nelle procedure di gara

1. Nelle procedure di affidamento di cui al D.lgs. 31 marzo 2023, n. 36 (c.d. Codice dei Contratti), l'Ateneo introduce criteri di valutazione premiali legati al livello di sicurezza dei fornitori e alla trasparenza della supply chain, per i casi previsti. Tali criteri possono includere elementi relativi alla provenienza dei componenti e alla localizzazione dei fornitori nonché al possesso di certificazioni di sicurezza informatica dei processi aziendali o dei prodotti o dei servizi erogati, con particolare attenzione a contesti che garantiscano adeguati standard di sicurezza, in coerenza con la tutela degli interessi strategici nazionali, come previsti dal D.P.C.M. 30 aprile 2025 e s.m.i..

## Art. 28 – Gestione dei rapporti contrattuali

1. Nell'ambito dei rapporti contrattuali con fornitori, partner e altri enti, l'Ateneo assicura che le relazioni aventi ad oggetto sistemi informativi, servizi digitali e trattamento dei dati siano disciplinate in coerenza con i principi di cybersicurezza e protezione dei dati personali, nel rispetto del quadro normativo vigente.

2. In caso di interconnessione tra sistemi dell'Ateneo e quelli di soggetti terzi, i contratti prevedono requisiti minimi di sicurezza, tra cui l'adozione di misure tecniche e organizzative adeguate e, ove applicabile, il possesso di certificazioni o standard equivalenti alla ISO/IEC 27001 per il contraente, al fine di garantire la protezione delle infrastrutture e la resilienza complessiva dei servizi interconnessi.

3. Nei casi di scambio di dati, i rapporti contrattuali disciplinano puntualmente le modalità di trattamento e protezione delle informazioni, prevedendo l'adozione di misure tecniche e organizzative adeguate.

4. La cooperazione applicativa tra enti pubblici è realizzata nel rispetto delle disposizioni di sicurezza di cui all'art. 50-ter del D.lgs. 82/2005 e s.m.i., garantendo l'interoperabilità dei sistemi, in condizioni di sicurezza e nel rispetto dei principi di integrità e riservatezza dei dati.

5. I contratti prevedono obblighi di collaborazione tra le parti in caso di incidenti significativi di sicurezza, anche potenziali, in coerenza con quanto previsto dall'art. 25 del D.lgs. 138/2024, nonché con le procedure interne adottate dall'Ateneo.

6. L'Ateneo promuove la sperimentazione e l'adozione progressiva di schemi contrattuali standardizzati in materia di cybersicurezza, suscettibili di aggiornamento in relazione all'evoluzione del quadro normativo e degli indirizzi emanati dalle autorità competenti, prevendendo clausole quali il recesso e risoluzione in caso di inadempienze o violazioni gravi della cybersicurezza.

## TITOLO IV - DISPOSIZIONI FINALI

### Art. 29 – Disposizioni finali

1. Per quanto non espressamente previsto dal presente regolamento si applicano le vigenti norme comunitarie, nazionali, statutarie e regolamentari in materia.

2. Gli allegati al presente regolamento non ne costituiscono parte integrante e sostanziale. Essi sono approvati e modificati con provvedimento del Direttore generale, nel rispetto delle prerogative sindacali, da assoggettarsi alle medesime forme di pubblicità previste per il regolamento.

3. Gli ulteriori documenti regolatori da adottarsi ai sensi della normativa in materia, quali, ad esempio, i Piani, sono approvati con il medesimo procedimento previsto per l'emanazione del presente regolamento.

4. Il presente regolamento è emanato con decreto del rettore ed è pubblicato nell'albo informatico dell'Ateneo, nonché sul relativo sito istituzionale. Entra in vigore dalla data indicata nel provvedimento rettorale di emanazione.

5. L'applicazione delle misure riportate nel presente regolamento avviene in conformità con le tempistiche previste dal Decreto NIS2 e dalle determinazioni dell'Agenzia Nazionale per la Cybersicurezza.

### All. 1 Politica di Classificazione degli Asset informatici

Si veda specifico allegato.

### All. 2 Politica per la Sicurezza degli asset informatici

Si veda specifico allegato.

### All. 3 Politica della sicurezza fisica

Si veda specifico allegato.

### All. 4 - Procedura di gestione degli incidenti

Si rimanda alla procedura adottata dal Consiglio di Amministrazione con delibera del 22 dicembre 2025 e s.m.i.; la procedura è disponibile sul portale di Ateneo all'indirizzo https://intranet.unige.it/notifica-incidenti-informatici.

### All. 5 - Glossario dei termini e riferimenti

## A

**ACN (Agenzia per la Cybersicurezza Nazionale):** Autorità nazionale italiana responsabile della cybersicurezza.

**AdS (Amministratori di Sistema):** Figure tecniche con privilegi elevati che gestiscono sistemi informatici.

**Asset:** Risorsa informatica di valore (hardware, software, attività e servizi ict, applicazioni, dati, reti).

**Autenticazione:** Processo di verifica dell'identità di un utente o sistema.

**Autorizzazione:** Processo di definizione dei permessi di accesso alle risorse informatiche.

## B

**Bill of Materials (BoM) / Software Bill of Materials (SBOM):** Elenco strutturato dei componenti hardware o software che costituiscono un sistema o applicazione, utile per la sicurezza e la tracciabilità.

## C

**CSIRT Italia (Computer Security Incident Response Team):** Struttura nazionale responsabile della gestione degli incidenti informatici significativi.

**Cybersecurity (Cybersicurezza):** Insieme di tecnologie e pratiche per proteggere sistemi, reti e dati.

**Classificazione degli asset:** Processo di categorizzazione delle risorse informatiche in base alla criticità.

**Common Security Framework 2.0** (CSF 2.0): Framework di riferimento per la gestione della sicurezza informatica basato su funzioni quali GOVERN, IDENTIFY e PROTECT, utilizzato per strutturare i processi di gestione del rischio cyber.

**Controllo degli accessi (Access Control):** Meccanismi che limitano l'accesso alle risorse informatiche.

**Ciclo di vita sicuro del software (Secure Software Lifecycle):** Approccio che integra la sicurezza in tutte le fasi di sviluppo del software.

## D

**Data (Dati):** Informazioni digitali trattate dai sistemi.

**Difesa in profondità (Defense in Depth):** Strategia di sicurezza basata su più livelli di protezione.

**DPIA:** Data Protection Impact Analysis, analisi di impatto del trattamento dati che viene svolta con il DPO nel caso di trattamenti che coinvolgano un numero elevato di interessati ed in presenza di rischi connessi alla tutela dei diritti di protezione dati degli interessati.

**Disaster Recovery:** Procedure per il ripristino dei sistemi dopo eventi critici.

## G

**GDPR (Regolamento (UE) 2016/679 - General Data Protection Regulation):** Regolamento europeo sulla protezione dei dati personali.

**Gestione del rischio (Risk Management):** Processo di identificazione, analisi e mitigazione dei rischi.

**Governo delle identità (Identity Governance):** Gestione e controllo delle identità digitali e dei relativi accessi.

## I

**ICT (Information and Communication Technology):** Tecnologie informatiche e di comunicazione.

**Identità digitale (Digital Identity):** Insieme delle informazioni che identificano un utente.

**Incident Response Team:** Gruppo incaricato della gestione degli incidenti informatici.

**Incidente informatico (Security Incident):** Evento che compromette la sicurezza dei sistemi.

**Integrità dei dati (Data Integrity):** Garanzia che i dati non siano alterati.

**ISO/IEC 27001 (Standard internazionale per la gestione della sicurezza delle informazioni):** Norma che definisce i requisiti per un sistema di gestione della sicurezza delle informazioni.

## M

**Minima esposizione:** Principio di sicurezza che riduce al minimo la superficie di attacco dei sistemi.

**Minimo privilegio (Least Privilege):** Principio secondo cui ogni utente ha solo i permessi necessari.

**Mitigazione del rischio (Risk Mitigation):** Azioni per ridurre probabilità o impatto dei rischi.

## N

**NIS2 (Direttiva (UE) 2022/2555 sulla sicurezza delle reti e dei sistemi informativi):** Direttiva europea sulla cybersicurezza.

## P

**Patch:** Aggiornamento software per correggere vulnerabilità.

**PIAO (Piano Integrato di Attività e Organizzazione):** Documento di pianificazione strategica delle PA.

**Protezione del dato (Data Protection):** Misure per garantire riservatezza, integrità e disponibilità dei dati.

**Piano di continuità operativa (Business Continuity Plan):** Piano per garantire la continuità dei servizi.

## R

**Rischio cyber (Cyber Risk):** Probabilità che una minaccia informatica causi un danno.

**Referenti Csirt:** soggetti incaricati di interloquire operativamente con il CSIRT Italia e con altre autorità di settore, anche al fine di effettuare le notifiche di incidente nei termini previsti dalla normativa vigente, in base alle direttive impartite dall'Incident Response Team

**Rete (Network):** Infrastruttura di comunicazione dei dati.

## S

**Segregazione delle reti (Network Segmentation):** Separazione delle reti per aumentare la sicurezza.

**Sistema informativo (Information System):** Insieme di risorse per la gestione delle informazioni.

**Sistemi di produzione (Production Systems):** Sistemi operativi in esercizio per servizi istituzionali.

**Sistemi di ricerca e sviluppo (R&D Systems):** Sistemi utilizzati per attività di ricerca e sperimentazione.

**Supply Chain:** Catena di fornitura di servizi e prodotti ICT.

**Software Open Source:** Software con codice sorgente accessibile.

## T

**Tracciabilità (Traceability):** Capacità di monitorare e registrare le attività.

## V

**Vulnerabilità (Vulnerability):** Debolezza di un sistema sfruttabile da minacce.