Università di Genova

Politica - Ruoli e responsabilità per la cybersecurity

Documento: GV_PO-01b – Versione 2.0 – 10 settembre 2026

Sommario

1 – Principi generali

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

3 – Organizzazione per la sicurezza informatica e filiera delle responsabilità

4 – Documentazione ed evidenze

5 – Revisione e approvazione

Università di Genova

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la chiara definizione dei ruoli, delle responsabilità e dei correlati poteri in materia di sicurezza informatica costituisce un presupposto essenziale per promuovere l'accountability, assicurare l'efficace gestione del rischio cyber e sostenere il miglioramento continuo delle misure di sicurezza. In tale prospettiva, l'organizzazione assicura che la propria struttura di sicurezza informatica sia formalmente definita, approvata dagli Organi di Amministrazione e Direttivi, resa nota alle articolazioni competenti e periodicamente riesaminata in coerenza con l'evoluzione del contesto organizzativo e di rischio.

Il riferimento organizzativo generale della presente politica è il Regolamento di Ateneo per la sicurezza informatica, che definisce l'organizzazione della sicurezza informatica e, nel Titolo I – Governance e responsabilità, disciplina la struttura organizzativa e i compiti dei diversi soggetti. In particolare, gli artt. 2–12 individuano gli attori della governance e ne articolano le funzioni direttive, di coordinamento, specialistiche e operative.

Il modello UniGe si fonda su un modello di responsabilità distribuita che coinvolge i vari attori responsabili: le responsabilità di indirizzo e supervisione degli Organi di Amministrazione e Direttivi si raccordano con le attività

- di coordinamento della Commissione per la Cybersicurezza, del Responsabile per la Transizione al Digitale (RTD), del Data Protection Officer (DPO), dell'Area ICT e dell'Incident Response Team;
- di tipo organizzativo dei dirigenti / soggetti assimilati, nonché dei Responsabili scientifici delle attività di didattica, ricerca o dei laboratori;
- di tipo tecnico ed operativo degli Amministratori di Sistema, dei suddetti Responsabili scientifici, dei Referenti CSIRT e degli altri soggetti individuati dal Regolamento.

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

Gli Organi di Amministrazione e direttivi NIS2 adottano indirizzi strategici e misure organizzative finalizzate a supportare i seguenti obiettivi:

- approvare l'organizzazione per la sicurezza informatica del soggetto NIS, stabilendone ruoli e responsabilità;
- adottare opportuni criteri per mantenere un elenco aggiornato del personale dell'organizzazione avente specifici ruoli e responsabilità in materia di sicurezza informatica e renderlo noto alle articolazioni competenti;
- assicurare che, all'interno dell'organizzazione per la sicurezza informatica, siano inclusi il punto di contatto NIS2 e il suo sostituto, i componenti dell'Incident Response Team, il referente CSIRT ed eventuali suoi sostituti, secondo quanto previsto dalle disposizioni applicabili;
- riesaminare e, se opportuno, aggiornare periodicamente ruoli e responsabilità e comunque almeno ogni due anni, nonché in occasione di incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.
- assicurare, in coerenza con gli artt. 3 e 5 del Regolamento di Ateneo per la sicurezza informatica, l'integrazione della cybersicurezza nei processi decisionali strategici, organizzativi e finanziari dell'Ateneo e l'assegnazione di risorse adeguate alle funzioni di presidio, coordinamento e risposta;
- istituire una struttura organizzativa preposta al presidio della cybersicurezza di Ateneo, promuovendone l'operatività e favorendo il potenziamento delle relative competenze professionali.

Università di Genova

3 – Organizzazione per la sicurezza informatica e filiera delle responsabilità

L'Ateneo definisce la propria organizzazione per la sicurezza informatica in modo formale, assicurandone l'approvazione da parte degli Organi di Amministrazione e Direttivi e la comunicazione alle articolazioni competenti del soggetto NIS. A supporto di tale assetto, l'organizzazione mantiene un elenco aggiornato del personale cui sono attribuiti specifici ruoli e responsabilità in materia di sicurezza informatica e include, all'interno della struttura così definita, il Punto di contatto dell'Ateneo rispetto all'agenzia ACN e il suo Sostituto, il Referente CSIRT e gli eventuali suoi sostituti, secondo quanto previsto dalla disciplina applicabile.

In coerenza col Regolamento di Ateneo per la sicurezza informatica, l'organizzazione è articolata secondo un modello di responsabilità distribuita nella quale si distinguono, senza creare compartimenti separati, funzioni direttive, funzioni di coordinamento e presidio specialistico e funzioni operative, come riportate nella tabella seguente.

Livello	Figure / riferimenti del Regolamento cybersicurezza	Responsabilità prevalente
Direttivo e strategico	Organi di Amministrazione e direttivi NIS2 – art. 3	Indirizzo, approvazione, supervisione, allocazione delle risorse e integrazione del rischio cyber nei processi decisionali.
Consultivo e di coordinamento	Commissione per la Cybersicurezza – art. 4; RTD e Area ICT – art. 5	Supporto alla governance; definizione delle priorità; coordinamento dell'attuazione delle politiche e raccordo tecnico-organizzativo con le strutture, gestione degli Incidenti.
Organizzativo di struttura	Dirigenti / soggetti assimilati; Responsabili scientifici delle attività di didattica, ricerca o dei laboratori – art. 6	Attuazione delle politiche, collaborazione alla redazione dei piani, validazione degli asset e presidio delle responsabilità nell'ambito della struttura.
Incidenti e compliance	Punto di Contatto, Incident Response Team, Referenti CSIRT – art. 8; DPO – art. 9	Gestione e notifica degli incidenti secondo le tempistiche previste da NIS2 e dal GDPR; raccordo con ACN/CSIRT/Garante Privacy; supporto per gli aspetti di protezione dei dati personali.
Scientifico-operativo	Responsabili scientifici delle attività di didattica, ricerca o dei laboratori – art. 7	Responsabilità sugli asset di ricerca e laboratorio: classificazione, valutazione del rischio, protezione e cooperazione costante con Area ICT e struttura.
Tecnico-operativo	Amministratori di Sistema – art. 10	Gestione tecnica dei sistemi, minimo privilegio, tracciabilità, continuità del

Livello	Figure / riferimenti del Regolamento cybersicurezza	Responsabilità prevalente
		censimento e caratterizzazione degli asset, attuazione delle misure di sicurezza.

Il presente modello andrà sviluppato con opportuni interventi organizzativi, come descritti al paragrafo 2.

Specificità del contesto Universitario

Il suddetto modello di responsabilità non si esaurisce nelle figure direttive e negli Amministratori di Sistema. In coerenza con l'art. 7 del Regolamento, i responsabili scientifici delle attività di didattica, ricerca o dei laboratori assumono specifiche responsabilità operative sugli asset di ricerca affidati o comunque riferibili alle attività scientifiche di competenza, cooperando alla classificazione degli asset, alla valutazione del rischio e all'adozione delle misure di protezione adeguate. Tale responsabilità è esercitata nel rispetto dell'autonomia scientifica e delle competenze organizzative delle strutture, secondo criteri di proporzionalità e gestione del rischio.

Amministratori di Sistema.

L'individuazione, la designazione, la gestione e il controllo degli Amministratori di Sistema sono disciplinati dalla specifica procedura, approvata dal Consiglio di amministrazione. La procedura integra i profili NIS2, AGID - CAD e di protezione dei dati personali e disciplina le diverse tipologie di AdS, i relativi ambiti di operatività, la tracciabilità, il monitoraggio e la cooperazione con le altre figure della filiera della cybersicurezza.

Struttura organizzativa per il presidio della cybersicurezza.

L'Ateneo persegue il progressivo potenziamento del presidio della cybersicurezza, istituendo un'apposita struttura organizzativa, intesa quale sistema coordinato di competenze, professionalità, presidi e funzioni specialistiche, con particolare riferimento all'Area ICT e alle strutture di supporto alla governance. L'Amministrazione provvede, in relazione all'evoluzione degli obblighi NIS2, dei rischi e delle esigenze dell'Ateneo, agli adeguamenti e alle evoluzioni organizzative necessari per assicurare adeguata capacità di prevenzione, gestione, risposta e miglioramento continuo.

Al fine di tutelare l'interesse pubblico connesso alla cybersicurezza e garantire la coerenza complessiva del modello, negli atti di organizzazione dell'Ateneo si tiene conto delle esigenze di adeguamento e sviluppo del sistema di governance della cybersicurezza, in conformità allo Statuto, ai regolamenti di Ateneo, alla disciplina applicabile alle università pubbliche e alla normativa in materia di pubblico impiego.

4 – Documentazione ed evidenze

Le attività svolte ai fini della definizione, assegnazione, comunicazione e revisione dei ruoli e delle responsabilità in materia di sicurezza informatica sono supportate da adeguata documentazione ed evidenze. Tale documentazione è conservata secondo le modalità definite dall'organizzazione, in modo da garantirne disponibilità, integrità e tracciabilità.

Rientrano tra le evidenze, secondo pertinenza: il Regolamento di Ateneo per la sicurezza informatica e i relativi documenti attuativi (ad es. Linee guida ict e Linee operative anche specifiche, ecc...); gli atti di designazione e organizzazione delle figure di riferimento per la direttiva NIS2 (es. elenchi aggiornati dei soggetti con specifiche responsabilità; nomine e archivi degli Amministratori di Sistema); le attribuzioni

riferite ai responsabili scientifici e agli asset di ricerca; gli atti di costituzione e aggiornamento di apposite strutture organizzative a presidio della cybersicurezza; i verbali, i piani, i report e le registrazioni che documentano l'esercizio delle responsabilità previste.

5 – Revisione e approvazione

La presente politica è approvata dagli Organi di Amministrazione e direttivi NIS2 ed entra in vigore alla data di adozione. La revisione avviene con cadenza programmata, a seguito di cambiamenti organizzativi/tecnologici/normativi significativi, o in seguito a incidenti di sicurezza.