Università di Genova

Politica - Sicurezza Fisica

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

Sommario

1 – Principi generali

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

3 – Protezione dell'accesso fisico

4 – Controllo e gestione degli accessi fisici

5 – Documentazione ed evidenze

6 – Revisione e approvazione

Università di Genova

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la protezione fisica dei sistemi informativi e di rete rilevanti costituisce una misura essenziale per prevenire accessi non autorizzati, manomissioni, furti, danneggiamenti e interruzioni dei servizi. A tal fine, l'organizzazione adotta misure organizzative e tecniche idonee a proteggere gli ambienti, le apparecchiature e le risorse fisiche che ospitano o supportano i sistemi informativi e di rete, in coerenza con la loro criticità e con il rischio cui sono esposti.

Per gli aspetti inerenti la salute e sicurezza dei lavoratori si rimanda alla normativa vigente, ai regolamenti dell'Ateneo ed alle specifiche procedure di sicurezza da esso previste, anche rispetto ai rischi specifici del contesto territoriale di UniGE. La presente politica è coordinata con i suddetti riferimenti normativi e regolamentari.

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:

- assicurare che, per almeno i sistemi informativi e di rete rilevanti, l'accesso fisico sia protetto mediante misure adeguate al rischio;
- garantire che l'accesso alle aree, ai locali e alle infrastrutture che ospitano asset critici sia consentito esclusivamente a soggetti autorizzati;
- promuovere l'adozione di regole di controllo, vigilanza e protezione degli ambienti fisici in cui sono collocati sistemi, apparati e supporti rilevanti;
- assicurare che le misure di sicurezza fisica siano coerenti con le esigenze di continuità operativa, protezione degli asset e gestione degli incidenti;
- garantire che siano adottate e documentate procedure a supporto della protezione dell'accesso fisico.

3 – Protezione dell'accesso fisico

Per almeno i sistemi informativi e di rete rilevanti, l'Ateneo assicura la protezione dell'accesso fisico ai locali, alle aree riservate, alle infrastrutture tecnologiche e agli apparati che ospitano o supportano tali sistemi. Le misure adottate sono definite in modo proporzionato alla criticità degli asset e possono comprendere, ove applicabili, controlli degli accessi agli ambienti, limitazioni agli ingressi, presidi organizzativi, misure di sorveglianza, protezione dei dispositivi e regolamentazione dell'accesso di personale interno, visitatori, manutentori e terze parti autorizzate.

La valutazione considera altresì, in funzione del rischio, minacce ambientali e accidentali quali incendio, allagamento, temperatura o umidità anomale, interruzione dell'alimentazione elettrica, danneggiamento e indisponibilità dei locali; le misure sono raccordate con i Piani di continuità operativa e di ripristino in caso di disastro previsti dal Regolamento di Ateneo per la Cybersicurezza.

4 – Controllo e gestione degli accessi fisici

L'Ateneo assicura che l'accesso fisico alle aree sensibili sia consentito solo per esigenze autorizzate e secondo modalità definite. Le autorizzazioni di accesso, le eventuali restrizioni, le regole di accompagnamento e le misure di controllo applicabili sono stabilite in coerenza con il livello di rischio, con la natura degli ambienti protetti e con le responsabilità dei soggetti ammessi. Le abilitazioni fisiche sono attribuite secondo il principio di necessità, riesaminate periodicamente e revocate senza ritardo quando cessano il ruolo o l'esigenza di accesso. Visitatori, manutentori e terze parti accedono secondo modalità autorizzate e, ove opportuno, accompagnate e tracciate.

In funzione della classificazione e del rischio dell'area, le misure possono comprendere:

- identificazione delle persone autorizzate e gestione controllata di chiavi, badge o altri dispositivi di accesso;
- registrazione degli accessi e conservazione delle evidenze per un periodo coerente con finalità, rischio e disciplina applicabile, in coerenza con le prescrizioni del Garante in materia di videosorveglianza, con i principi di limitazione della conservazione, in coerenza con l'accordo di Ateneo relativo alla videosorveglianza.
- regole per consegne, interventi tecnici, permanenza di terzi e rimozione o movimentazione di apparati e supporti;
- verifica periodica del corretto funzionamento dei presidi fisici e segnalazione tempestiva di anomalie, smarrimenti, effrazioni o accessi non autorizzati.

5 – Documentazione ed evidenze

Le attività svolte ai fini della sicurezza fisica 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.

Le evidenze comprendono, ove applicabili, elenchi delle persone autorizzate, verbali o registri di consegna di chiavi e badge, log di accesso, registri dei visitatori e degli interventi manutentivi, esiti delle verifiche sui presidi e informazioni di censimento relative ai locali protetti. L'accesso a tali evidenze è limitato ai soggetti autorizzati e avviene nel rispetto delle prerogative dello Statuto dei lavoratori, della normativa in materia di protezione dei dati personali e delle altre norme applicabili.

Ogni evento fisico che abbia compromesso o possa compromettere disponibilità, integrità, autenticità o riservatezza di sistemi, dati o servizi ICT è segnalato tempestivamente attraverso i canali previsti dalla procedura di gestione degli incidenti approvata dal Consiglio di amministrazione, ferma restando l'attivazione delle ulteriori procedure di Ateneo eventualmente applicabili all'evento.

6 – 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.

Il riesame tiene conto anche degli esiti del censimento degli asset, delle analisi del rischio, degli audit, dei test di continuità operativa e delle anomalie o degli eventi fisici registrati.