Università di Genova

Politica - Conformità e Audit di Cybersecurity

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

Sommario

1 – Principi generali

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

3 – Adozione, riesame e adeguamento delle politiche

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 conformità e l'audit di sicurezza costituiscono elementi essenziali per assicurare che le politiche di sicurezza informatica siano formalmente adottate, correttamente applicate e mantenute nel tempo in coerenza con l'evoluzione del contesto normativo, organizzativo e di rischio. In tale prospettiva, l'organizzazione assicura che le politiche siano approvate dagli Organi di Amministrazione e Direttivi, rese note alle articolazioni competenti del soggetto NIS, secondo il principio del *need to know* e periodicamente riesaminate, così da verificarne la conformità alla normativa applicabile e individuare gli eventuali interventi di adeguamento necessari. La presente politica si colloca nel quadro del Regolamento di Ateneo per la sicurezza informatica, che disciplina la governance, le responsabilità e i processi di gestione, monitoraggio e miglioramento della cybersicurezza dell'Ateneo.

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:

- adottare politiche di sicurezza informatica per gli ambiti previsti dalle misure applicabili;
- assicurare che tali politiche includano almeno i requisiti previsti per i relativi ambiti;
- garantire che le politiche siano approvate e rese note alle articolazioni competenti del soggetto NIS tenendo conto del need to know;
- assicurare che le politiche siano riesaminate e, se opportuno, aggiornate periodicamente, nonché a fronte di evoluzioni normative, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi;
- verificare, in sede di riesame, almeno la conformità delle politiche alla normativa in materia di sicurezza informatica;
- approvare un piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza;
- verificare l'attuazione delle opportune iniziative di comunicazione ai soggetti interessati circa gli esiti dei piani di adeguamento mediante apposite relazioni.
- assicurare che gli esiti delle attività di audit e monitoraggio siano utilizzati per il miglioramento continuo del processo di gestione del rischio cyber e delle misure di sicurezza adottate, in coerenza con il Regolamento di Ateneo per la sicurezza informatica.

3 – Adozione, riesame e adeguamento delle politiche

L'Ateneo adotta e documenta politiche di sicurezza informatica per gli ambiti previsti dalle misure applicabili, assicurando che esse includano almeno i requisiti richiesti e siano approvate dagli Organi di Amministrazione e Direttivi. Tali politiche sono rese note alle

articolazioni competenti del soggetto NIS secondo il principio del need to know e sono riesaminate periodicamente, nonché ogniqualvolta si verifichino evoluzioni del contesto normativo, incidenti significativi, variazioni organizzative o mutamenti dell'esposizione alle minacce e ai relativi rischi.

In esito al riesame, l'organizzazione verifica almeno la conformità delle politiche alla normativa in materia di sicurezza informatica e, ove necessario, definisce e attua un piano di adeguamento che individua gli interventi necessari ad assicurarne l'effettiva attuazione; gli esiti di tali attività sono portati all'attenzione degli Organi di Amministrazione e Direttivi mediante apposite relazioni periodiche.

La predisposizione e l'aggiornamento delle politiche sono coordinati dalla Commissione per la Cybersicurezza e dal Responsabile per la Transizione Digitale (RTD), attraverso l'Area ICT e il relativo Ufficio di supporto, con la collaborazione dei dirigenti e degli altri soggetti competenti, secondo il modello organizzativo definito dal Regolamento Cybersicurezza. Le attività di audit e monitoraggio costituiscono inoltre una fase del processo di gestione del rischio e si applicano, secondo criteri di adeguatezza, proporzionalità e valutazione del rischio, a tutte le strutture dell'Ateneo, inclusi i contesti di ricerca e sviluppo.

4 – Documentazione ed evidenze

Le attività svolte ai fini della conformità e degli audit di sicurezza 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.

Qualora le evidenze comprendano log o registrazioni di sicurezza, il relativo accesso, utilizzo e conservazione avvengono nel rispetto delle finalità, delle autorizzazioni e delle garanzie previste dallo Statuto dei lavoratori, dalla normativa in materia di trattamento dei dati personali, dal Regolamento di Ateneo per la sicurezza informatica e dall'ulteriore normativa applicabile.

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.

Il riesame tiene altresì conto degli esiti degli audit, del monitoraggio, delle valutazioni del rischio e degli eventuali piani di adeguamento, in coerenza con il sistema di governance della cybersicurezza di Ateneo.