Università di Genova

Politica – Affidabilità Risorse Umane

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

Sommario

1 – Principi generali

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

3 – Personale autorizzato e amministratori di sistema

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 l'affidabilità delle risorse umane costituisce un elemento essenziale per la protezione dei sistemi informativi e di rete e per la corretta attuazione delle misure di sicurezza informatica. In tale prospettiva, l'organizzazione assicura che l'accesso ad infrastrutture ict / sistemi ict rilevanti e l'attribuzione di privilegi amministrativi siano consentiti soltanto a personale la cui esperienza, capacità e affidabilità siano state preventivamente valutate in modo coerente con la criticità dei sistemi, con il livello di accesso attribuito e con le responsabilità connesse al ruolo.

La presente Policy è attuata in coerenza con il Regolamento di Ateneo per la sicurezza informatica, con il D.lgs. 4 settembre 2024, n. 138 di recepimento della Direttiva NIS2, con il Regolamento (UE) 2016/679 (GDPR), il Regolamento privacy UniGE e i provvedimenti del Garante per la protezione dei dati personali.

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 tutto il personale autorizzato ad accedere ai sistemi informativi e di rete rilevanti sia individuato previa valutazione della relativa esperienza, capacità e affidabilità, nonché dell'adeguatezza rispetto alle funzioni effettivamente svolte e al livello di accesso richiesto, anche per mezzo di adeguate politiche di formazione, in raccordo con la *Politica - Formazione del personale e consapevolezza* e al *Piano di formazione di Ateneo in tema di protezione dei dati personali*;
- garantire che gli amministratori di sistema siano individuati previa analoga valutazione, secondo la specifica Procedura per la nomina e gestione degli Amministratori di Sistema adottata dal Consiglio di amministrazione, coerente con la disciplina NIS2, con il GDPR e con il Provvedimento del Garante del 27 novembre 2008 e s.m.i..

3 – Personale autorizzato e amministratori di sistema

Per almeno i sistemi informativi e di rete rilevanti, l'Ateneo individua il personale autorizzato ad accedervi previa valutazione dell'esperienza, delle capacità e dell'affidabilità del soggetto interessato. Analoga valutazione è svolta per gli amministratori di sistema dei sistemi informativi e di rete, in considerazione dei privilegi amministrativi a loro attribuiti.

Nei processi valutativi e selettivi, nell'ambito dell'accertamento delle competenze informatiche, si tiene conto anche degli aspetti di cybersicurezza.

4 – Documentazione ed evidenze

Le attività svolte ai fini dell'affidabilità delle risorse umane 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.

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 considera inoltre l'evoluzione del perimetro NIS2, delle procedure di gestione degli Amministratori di Sistema e del modello di governo delle identità e degli accessi ordinari in coerenza con la Policy GV_PO-01i_Policy_Accessi_Identità.