Università di Genova

Politica - Gestione dell'autenticazione, delle identità digitali e del controllo accessi

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

Sommario

1 – Principi generali
2 – Impegni degli Organi di Amministrazione e Direttivi NIS2
3 – Gestione delle identità digitali
4 – Autenticazione, autorizzazioni e controllo degli accessi
5 – Documentazione ed evidenze
6 – Revisione e approvazione

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la gestione delle identità digitali, dell'autenticazione e delle autorizzazioni di accesso costituisce una misura fondamentale per proteggere i sistemi informativi e di rete da accessi non autorizzati, utilizzi impropri, escalation di privilegi e compromissioni delle credenziali. A tal fine, l'organizzazione adotta misure organizzative e tecniche volte a garantire che l'accesso agli asset e ai sistemi sia consentito esclusivamente a utenti, servizi e dispositivi autorizzati, in modo coerente con il rischio, con il ruolo ricoperto e i principi con need to know, minimo privilegio e separazione delle funzioni.

La presente Policy dà attuazione al Regolamento di Ateneo per la cybersicurezza, assicurando la riconducibilità certa dell'identità digitale, il governo degli accessi, la responsabilità nell'uso dell'identità e il monitoraggio e la tracciabilità.

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 tutte le utenze, incluse quelle con privilegi amministrativi e quelle utilizzate per l'accesso remoto, siano censite, approvate e gestite secondo regole definite;
- garantire che le modalità di autenticazione siano commisurate al rischio e che, per almeno i sistemi informativi e di rete rilevanti, siano adottate adeguate soluzioni di autenticazione, ad es. tramite l'utilizzo della Multi Factor Authentication (MFA);
- assicurare che i permessi di accesso siano assegnati e riesaminati in accordo ai principi del minimo privilegio, della segmentazione, della separazione delle funzioni e del principio del need to know;
- promuovere la revisione periodica delle utenze e delle relative autorizzazioni, nonché il tempestivo aggiornamento o la revoca degli accessi in caso di variazioni organizzative o cessazioni;
- garantire che siano definite e documentate le attività consentite da remoto, e le relative modalità di accesso, e che sia mantenuto un elenco aggiornato dei sistemi informativi e di rete ai quali è possibile accedere da remoto.

3 – Gestione delle identità digitali

Gestione Identità digitali - Tutte le identità digitali (in seguito anche "identità") utilizzate per accedere ai sistemi informativi e di rete dell'organizzazione, incluse quelle privilegiate e quelle abilitate all'accesso remoto, sono censite, approvate dagli Amministratori di Sistema e, fatte salve motivate e documentate ragioni tecniche, assegnate in forma individuale agli utenti. Le credenziali associate alle identità sono definite e mantenute secondo criteri di robustezza e aggiornamento coerenti con il livello di rischio e con la criticità dei sistemi cui consentono l'accesso. Il ciclo di vita dell'identità comprende fasi

quali: i) richiesta e approvazione, ii) attivazione, iii) modifica, iv) riesame periodico, v) sospensione o revoca.

Variazioni di ruolo, struttura o rapporto con l'Ateneo devono produrre il tempestivo adeguamento o deprovisioning degli accessi.

Le autorizzazioni sono attribuite sulla base delle esigenze istituzionali e del ruolo effettivamente svolto, in coerenza con la policy GV_PO-01c_Policy_Risorse_Umane.

Per gli ambiti amministrativi, didattici, di ricerca e di laboratorio, i responsabili competenti concorrono all'individuazione degli accessi necessari e alla loro periodica conferma, in coerenza con la classificazione e la criticità degli asset e dei dati trattati.

Identità applicative - Le identità tecniche, di servizio, applicative o macchina devono avere un titolare organizzativo e un responsabile tecnico identificabili, finalità documentata, privilegi limitati e credenziali protette. Le utenze condivise sono ammesse solo quando tecnicamente inevitabili, previa motivazione e adozione di misure che garantiscano imputabilità e tracciabilità dell'utilizzo.

Identità Amministrative - Per le utenze con privilegi elevati si applicano le prassi del Regolamento di Ateneo per la sicurezza informatica e la Procedura di Ateneo per gli Amministratori di Sistema: designazione individuale, distinzione tra utenza ordinaria e amministrativa, credenziali separate, ambito di operatività definito, verifica della permanenza dei requisiti e revoca tempestiva dei privilegi non più necessari.

4 – Autenticazione, autorizzazioni e controllo degli accessi

Autenticazione - Le modalità di autenticazione adottate dall'organizzazione per accedere ai sistemi informativi e di rete sono commisurate al rischio, tenendo conto almeno dei privilegi associati alle utenze, della criticità dei sistemi e della tipologia di operazioni consentite; per almeno i sistemi informativi e di rete rilevanti, in coerenza con gli esiti della valutazione del rischio, sono impiegate soluzioni di autenticazione avanzate, come ad es. quelle multi-fattore.

Autorizzazione - I permessi, i diritti e le autorizzazioni di accesso sono assegnati e gestiti in accordo ai principi del minimo privilegio, della separazione delle funzioni e del need to know, assicurando la distinzione tra utenze ordinarie e utenze con privilegi amministrativi. Le eventuali attività consentite da remoto sono definite e documentate; è mantenuto un elenco aggiornato dei sistemi ai quali è possibile accedere da remoto, con indicazione delle relative modalità di accesso, e le autorizzazioni sono verificate periodicamente, aggiornandole o revocandole in caso di variazioni organizzative o cessazioni.

I sistemi di autenticazione multi-attore (es. MFA) sono adottati in modo diffuso, ove tecnicamente opportuno e possibile, prioritariamente per le utenze privilegiate, per l'accesso remoto, per i servizi esposti su Internet e per i sistemi o servizi rilevanti. L'estensione agli ulteriori sistemi avviene secondo la valutazione del rischio, la fattibilità tecnica e un piano di adeguamento documentato; eventuali eccezioni devono essere

motivate, approvate dal responsabile competente, riesaminate periodicamente e accompagnate da misure compensative.

Gli accessi di fornitori e soggetti esterni sono nominativi, limitati per durata e ambito, autorizzati dal responsabile competente e disabilitati al termine dell'attività.

Gli eventi di autenticazione, le modifiche dei privilegi e le attività amministrative sono registrati e monitorati in coerenza con il Regolamento di Ateneo per la Cybersicurezza, nel rispetto delle disposizioni previste nello Statuto dei lavoratori e dalla normativa in materia di trattamento dei dati personali. Gli accessi anomali o sospetti sono gestiti secondo il Piano di gestione degli incidenti informatici dell'Ateneo.

5 – Documentazione ed evidenze

Le attività svolte ai fini della gestione dell'autenticazione, delle identità digitali e del controllo accessi 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 applicabile, richieste e approvazioni, inventari delle utenze, titolari e ruoli, esiti dei riesami, revoche, sistemi accessibili da remoto e registrazioni degli eventi rilevanti.

La Policy è coordinata con il Regolamento di Ateneo in materia di sicurezza informatica, con la Procedura per gli Amministratori di Sistema e con le altre policy e procedure di gestione del rischio, degli asset, dei log e degli incidenti.

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 o normativi significativi, o in seguito a incidenti di sicurezza.