Università di Genova

# Politica - Gestione degli Asset ICT

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

# Sommario

1 – Principi generali
2 – Impegni degli Organi di Amministrazione e Direttivi NIS2
3 – Inventario degli asset ICT rilevanti
4 – Classificazione dei sistemi e supporto all'analisi del rischio
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 corretta identificazione e gestione–degli asset[1] costituisce un presupposto essenziale per la protezione dei sistemi informativi e di rete e per l'efficace attuazione delle misure di sicurezza informatica. In tale prospettiva, l'organizzazione assicura la costante conoscenza e tracciabilità degli apparati fisici, dei servizi, dei sistemi, delle applicazioni software e dei servizi informatici erogati dai fornitori che compongono o supportano i sistemi informativi e di rete rilevanti, così da consentire una gestione coerente con la loro criticità e con il rischio associato.

# 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 il mantenimento di un censimento aggiornato di reti informatiche, sistemi informativi rilevanti[2], attività e servizi ict, identità digitali;
- estendere progressivamente, in una seconda fase e sulla base della rilevanza rispetto al rischio, la mappatura ad ulteriori categorie di asset, quali dispositivi IoT, OT, mobili ed endpoint secondo un criterio di gradualità.

# 3 – Inventario degli asset ICT rilevanti

L'Ateneo assicura il mantenimento di inventari aggiornati degli asset che compongono o supportano i sistemi informativi e di rete, quali presupposti essenziali per la loro corretta gestione e per l'attuazione delle misure di sicurezza informatica.

In prima applicazione, il perimetro dell'inventario comprende:

- Reti informatiche: tutte le reti di Ateneo, indipendentemente dal livello di criticità, incluse WAN, MAN, LAN, VLAN, VXLAN, che siano fisiche o logiche, cablate o wireless, compresi tutti i relativi apparati di rete;
- Sistemi informativi rilevanti:
    - On-premise - server fisici e virtuali ospitati nelle infrastrutture dell'Ateneo, applicazioni e componenti che erogano o supportano servizi digitali;
    - Cloud - sistemi e piattaforme erogati tramite fornitori esterni, inclusi servizi IaaS, PaaS e SaaS;
- Attività e Servizi iCT: servizi digitali erogati agli utenti interni o esterni, con indicazione delle finalità, dei destinatari e delle dipendenze da reti, sistemi e fornitori.

[1] Per asset si intendono a titolo esemplificativo e non esaustivo: reti, sistemi, dispositivi, identità digitali, attività e servizi digitali, applicazioni, archivi di dati strutturati o non strutturati.

[2] Si definiscono rilevanti i sistemi la cui la perdita anche temporanea di disponibilità e/o integrità, e/o autenticità e/o riservatezza può arrecare pregiudizio alle attività istituzionali dell'Ateneo.

- Identità digitali (relative a persone fisiche o applicative).

In conformità alle disposizioni NIS2 l'Ateneo provvede a comunicare all'Autorità l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi.

A tendere l'inventario è esteso alle ulteriori categorie di asset previste dalla presente politica — in particolare dispositivi IoT, OT, mobili ed endpoint — quando la loro criticità, esposizione, interconnessione o tipologia di dati trattati ne determini la rilevanza ai fini del rischio cyber.

## 4 – Classificazione dei sistemi e supporto all'analisi del rischio

I sistemi di rete e i sistemi informativi rilevanti on-premise e cloud sono censiti e caratterizzati mediante attributi omogenei, utilizzati come base conoscitiva per l'analisi del rischio e per la definizione delle priorità di trattamento. In particolare, la caratterizzazione considera in prima applicazione:

- la struttura di riferimento, il responsabile, i referenti tecnici e gli amministratori del sistema;
- l'ubicazione o il modello di erogazione, la natura fisica o virtuale, la piattaforma, il fornitore e le dipendenze ICT;
- la finalità istituzionale, i servizi erogati, i destinatari, l'esposizione verso l'esterno e le interconnessioni con altri sistemi o reti;
- le politiche di protezione attuate;
- il livello di criticità dei dati trattati, personali e non personali. Sono considerati, con gradualità crescente, dati comuni e istituzionali, dati personali, categorie particolari di dati personali, dati giudiziari, dati biometrici, genetici e sanitari, nonché ogni ulteriore dato la cui perdita di disponibilità, integrità, autenticità o riservatezza possa arrecare pregiudizio alle funzioni istituzionali dell'Ateneo. Tali categorie sono riportate nella policy GV_PO-01l_Policy_Sicurezza_Dati.

Il modello di gestione dei sistemi, con relativi dati gestiti, approvato con la delibera del Consiglio di Amministrazione n. 275 del 26 novembre 2025 e s.m.i., costituisce il riferimento iniziale per tale classificazione. Il rischio è determinato considerando il dato più critico trattato in un dato sistema, unitamente a esposizione, numerosità e tipologia degli utenti, finalità del servizio, interconnessioni e dipendenze da infrastrutture o fornitori.

Posto che l'archivio degli asset può contenere sistemi, attività o servizi che contengono categorie particolari di dati (art. 9 GDPR) o dati giudiziari (art. 10 GDPR) l'archivio è condiviso con il DPO, al fine di consentirgli di valutare la necessità di DPIA e di aggiornare il Registro dei Trattamenti.

## 5 – Documentazione ed evidenze

Le attività svolte ai fini della gestione degli asset 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.

Gli inventari sono aggiornati in modo continuativo mediante un sistema informativo il più possibile integrato a livello delle diverse dimensioni previste (es. ruoli, asset, anagrafiche, sedi, ecc…). Le strutture competenti assicurano la validazione periodica dei dati e

l'aggiornamento a seguito di variazioni significative di reti, sistemi, servizi, fornitori o modalità di trattamento dei dati.

## 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.