Università di Genova

Politica - Gestione dei rischi per la cybersecurity della catena di approvvigionamento

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

Sommario

1 – Principi generali

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

3 – Governance delle forniture

4 – Requisiti di sicurezza

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 i rischi derivanti da fornitori, prodotti, servizi e altre terze parti possono incidere in modo significativo sulla sicurezza dei sistemi informativi e di rete e sulla continuità dei servizi erogati. In tale prospettiva, l'organizzazione assicura che i processi di approvvigionamento e di gestione delle forniture con potenziali impatti sulla sicurezza informatica siano disciplinati secondo un approccio basato sul rischio, che tenga conto della criticità della fornitura, del livello di accesso ai sistemi e ai dati, dell'impatto di eventuali interruzioni e delle responsabilità attribuite al fornitore nel governo dei sistemi e dei servizi.

La presente Policy attua e specifica, per gli aspetti operativi, i principi del Regolamento di Ateneo per la sicurezza informatica inerente la supply chain ICT.

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 coinvolgimento dell'organizzazione per la sicurezza informatica nella definizione ed esecuzione dei processi di approvvigionamento ICT fin dalla fase di identificazione e progettazione della fornitura;
- garantire che, in accordo con gli esiti della valutazione del rischio associato alla fornitura, siano definiti requisiti di sicurezza coerenti con le misure di sicurezza applicate dall'organizzazione ai propri sistemi informativi e di rete;
- definire e rendere noti alle articolazioni competenti del soggetto NIS gli eventuali ruoli e responsabilità in materia di sicurezza informatica assegnati al personale delle terze parti;
- mantenere un inventario aggiornato dei fornitori delle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete;
- assicurare che i requisiti di sicurezza siano inseriti, fatte salve motivate e documentate ragioni normative o tecniche, nelle richieste di offerta, nei bandi di gara, nei contratti, negli accordi e nelle convenzioni relativi alle forniture rilevanti[1];
- promuovere, nei casi applicabili, l'inserimento nelle procedure di gara di criteri di valutazione premiali connessi al livello di sicurezza del fornitore e alla trasparenza della catena di approvvigionamento;
- garantire che il rischio associato alle forniture sia valutato, documentato, monitorato e riesaminato nel corso della relazione contrattuale, nonché che sia verificata periodicamente e documentata la conformità delle forniture ai requisiti di sicurezza definiti;

[1] La rilevanza delle forniture ICT si inquadra nell'ambito di acquisizione di beni, servizi o progettazione di lavori finalizzati ad aggiornare o mettere in esercizio asset informatici rilevanti per l'assolvimento delle attività istituzionali dell'Ateneo.

- assicurare che contratti, accordi e convenzioni che comportino l'erogazione di servizi ICT o l'accesso a sistemi e dati dell'Ateneo contengano obblighi di cooperazione e tempestiva comunicazione in caso di incidenti informatici, idonei a consentire all'Ateneo l'adempimento degli obblighi di cui all'art. 25 del D.lgs. 138/2024 e l'attivazione della propria Procedura di gestione e notifica degli incidenti.

3 – Governance delle forniture

In merito all'affidamento di forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, l'Ateneo prevede il coinvolgimento dell'organizzazione per la sicurezza informatica nella definizione ed esecuzione dei processi di approvvigionamento fin dalla fase di identificazione e progettazione della fornitura.

Le strutture competenti per l'approvvigionamento e i responsabili di progetto coinvolti (RUP) assicurano il raccordo col Regolamento di Ateneo per la cybersicurezza in ordine alla sicurezza della supply chain ICT; a tale fine l'Area ICT rende disponibili linee guida sulle nuove tecnologie da adottare che costituiscono un primo quadro di riferimento; a tale fine l'Area ICT svolge un ruolo consultivo e di indirizzo.

Le medesime esigenze di sicurezza si applicano, per quanto compatibili, anche ai rapporti di cooperazione, partenariato, consorzio o collaborazione che comportino interconnessione di sistemi, condivisione di servizi ICT o trattamento/scambio di dati. Negli accordi tra Pubbliche Amministrazioni, gli obblighi di cooperazione in materia di cybersicurezza e di comunicazione degli incidenti sono definiti in forma reciproca, secondo le rispettive responsabilità e il rischio connesso alle attività condivise.

Ai fini del governo della supply chain ICT, è inoltre previsto il presidio e lo sviluppo progressivo di linee guide e prassi volte al miglioramento della supply chain, tra cui:

- identificazione dei fornitori rilevanti NIS[2] e comunicazione degli stessi all'Autorità NIS. In prima applicazione la comunicazione può riguardare operatori economici di forniture relative alle infrastrutture ed ai servizi ICT centrali;

- criteri documentati di criticità, fungibilità e concentrazione;

- due diligence prima dell'affidamento e riesame durante il rapporto;

- requisiti selezionati in funzione del rischio, con motivazione della selezione;

- diritto di audit presso i fornitori, evidenze di conformità e gestione delle non conformità;

- obblighi a cascata verso subfornitori, subappaltatori e subcontraenti;

- restituzione/cancellazione dei dati, revoca degli accessi e piano di uscita;

- gestione di lock-in.

[2] Cfr. nota precedente

4 – Requisiti di sicurezza

L'Ateneo mantiene un inventario aggiornato dei fornitori delle forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete rilevanti. In accordo con gli esiti della valutazione del rischio associato alla fornitura, sono definiti requisiti di sicurezza coerenti con le misure adottate dall'organizzazione e fatte salve motivate e documentate ragioni normative o tecniche, tali requisiti sono inseriti nella documentazione di gara, nei contratti, negli accordi e nelle convenzioni applicabili.

Il rischio associato alle forniture è valutato e documentato tenendo conto almeno del livello di accesso del fornitore ai sistemi informativi e di rete, dell'accesso alla proprietà intellettuale e ai dati in relazione alla loro criticità, dell'impatto di una grave interruzione della fornitura, dei tempi e dei costi di ripristino in caso di indisponibilità dei servizi e dei ruoli e delle responsabilità del fornitore nel governo dei sistemi informativi e di rete; la conformità delle forniture ai requisiti di sicurezza definiti è verificata periodicamente e documentata.

In coerenza col Regolamento di Ateneo, i requisiti devono inoltre consentire, ove pertinente, la ricostruibilità e la tracciabilità dei componenti che costituiscono la fornitura o il servizio e la trasparenza sui subfornitori, subappaltatori e subcontraenti.

4.1 – Requisiti nelle procedure di affidamento

Nelle procedure di affidamento di beni e servizi ICT, in relazione alla natura e al livello di rischio della fornitura, la documentazione di gara individua requisiti minimi e, ove previsto, criteri premiali di cybersicurezza. In coerenza col Regolamento di Ateneo, possono essere valorizzati, a titolo esemplificativo: certificazioni o attestazioni di sicurezza pertinenti; processi di gestione delle vulnerabilità e degli aggiornamenti; continuità operativa; tracciabilità della catena di fornitura, disponibilità di ulteriori dettagli correlati alla specifica natura dell'affidamento.

4.2 – Clausole contrattuali per incidenti e cooperazione

I contratti, gli accordi, le convenzioni e gli altri strumenti negoziali relativi a forniture o servizi ICT rilevanti prevedono specifiche clausole che obbligano il fornitore, il consorziato, il partner o altro soggetto terzo a segnalare senza ingiustificato ritardo all'Ateneo qualsiasi incidente, anche potenziale, che possa incidere sui sistemi, sui servizi o sui dati dell'Università.

La comunicazione deve avvenire con tempestività sufficiente a consentire all'Ateneo di valutare la significatività dell'evento, attivare l'Incident Response Team e i Referenti CSIRT e rispettare, ove applicabili, le tempistiche di notifica previste dall'art. 25 del D.lgs. 138/2024 e dalla Procedura di Ateneo di gestione e notifica degli incidenti. Il soggetto terzo coopera inoltre nelle attività di contenimento, analisi, raccolta delle evidenze, ripristino, aggiornamento informativo e predisposizione delle comunicazioni richieste dalle autorità competenti.

Per gli accordi tra Pubbliche Amministrazioni le clausole sono formulate in termini di obbligo reciproco di tempestiva informazione e cooperazione in caso di incidente che possa propagarsi o produrre effetti sui sistemi, sui servizi o sui dati dell'altra

amministrazione. Restano ferme le autonome responsabilità di ciascuna amministrazione rispetto agli obblighi di notifica ad essa applicabili.

4.3 – Servizi cloud e altri servizi esternalizzati

Gli obblighi di cui al presente articolo si applicano anche ai servizi cloud e, più in generale, ai servizi esternalizzati o gestiti da terzi, inclusi i casi in cui l'infrastruttura non sia fisicamente collocata presso l'Ateneo. Nei rapporti contrattuali sono disciplinati, in modo proporzionato al rischio, almeno i canali e i referenti per la segnalazione degli incidenti, i tempi di comunicazione, l'accesso alle informazioni utili all'analisi, la gestione delle vulnerabilità, la continuità e il ripristino, la subfornitura e le modalità di uscita o migrazione dal servizio.

5 – Documentazione ed evidenze

Le attività svolte ai fini della gestione dei rischi per la sicurezza informatica della catena di approvvigionamento 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, la documentazione richiamata al par 4.1.

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 considera altresì l'evoluzione delle disposizioni e degli indirizzi ACN in materia di supply chain, delle regole applicabili ai contratti pubblici e delle prassi di Ateneo relative alla gestione degli incidenti e alla sicurezza dei fornitori.