Università
Iuav
di Venezia

REGOLAMENTO PER L'ORGANIZZAZIONE DELLA SICUREZZA INFORMATICA

(emanato con decreto rettorale del 18 maggio 2026 n. 302)

INDICE

TORNA ALL'INDICE

Articolo 1
(Finalità e ambito di applicazione)

Il presente regolamento definisce i ruoli, le responsabilità e le autorità relative alla gestione della sicurezza informatica nell'ambito dell'Università Iuav di Venezia, in attuazione degli obblighi derivanti dalla Direttiva (UE) 2022/2555 (NIS 2), dal decreto legislativo 4 settembre 2024 n. 138 e dalla determina dell'Agenzia per la Cybersicurezza Nazionale - ACN 14 aprile 2025 n. 164179.
L'ateneo, classificato come "soggetto importante" ai sensi della normativa richiamata, è tenuto a dotarsi di un'organizzazione formalmente strutturata per la gestione della sicurezza informatica, che assicuri una chiara attribuzione delle responsabilità, l'assenza di vuoti di governo e la piena tracciabilità delle decisioni in materia.
Il presente regolamento si applica agli organi di governo, alle strutture amministrative, ai dipartimenti, ai centri e a qualsiasi altra articolazione organizzativa dell'ateneo, nonché al personale tecnico-amministrativo, docente e ai collaboratori esterni che operano sui sistemi informativi e di rete dell'Università.

Articolo 2
(Riferimenti normativi)

- Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio (NIS 2)
- decreto legislativo 4 settembre 2024 n. 138 - recepimento della Direttiva NIS 2
- determina Agenzia per la Cybersicurezza Nazionale - ACN 14 aprile 2025 n. 164179
- statuto dell'Università IUAV di Venezia
- regolamento generale di ateneo
- decreto legislativo 30 marzo 2001 n. 165 - Ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche
- regolamento (UE) 2016/679 (GDPR)
- Framework Nazionale per la Cybersecurity (FNCS) - ACN

Articolo 3
(Principi generali)

L'organizzazione per la sicurezza informatica dell'ateneo si fonda sui seguenti principi:
1. Responsabilità distribuita e non delegabile. La sicurezza informatica è una responsabilità condivisa a tutti i livelli dell'organizzazione. Ciascun ruolo individuato nel presente Regolamento risponde delle proprie attribuzioni in modo diretto e non può delegarle integralmente ad altri soggetti.
2. Proporzionalità. Le misure e i processi di governance della sicurezza informatica sono proporzionati alla natura, alla dimensione e al profilo di rischio dell'ateneo, tenendo conto delle specificità del contesto universitario pubblico.
3. Integrazione con la governance di ateneo. La sicurezza informatica è parte integrante della governance complessiva dell'ateneo e si raccorda con i processi di gestione del rischio istituzionale, di programmazione strategica e di controllo interno.
4. Continuità e aggiornamento. L'organizzazione per la sicurezza informatica è oggetto di riesame periodico per garantirne l'adeguatezza rispetto all'evoluzione delle minacce, della tecnologia e dell'assetto organizzativo dell'ateneo.

Articolo 4
(Struttura organizzativa per la sicurezza informatica)

4.1 **Consiglio di amministrazione**

Il consiglio di amministrazione è l'organo di indirizzo strategico e di supervisione in materia di sicurezza informatica. In tale veste:
- approva il presente regolamento e i suoi aggiornamenti;
- approva la policy di sicurezza informatica dell'ateneo e le sue revisioni periodiche;

- approva il Piano di gestione dei rischi di natura informatica e il relativo piano di trattamento;
- approva il Piano di adeguamento NIS 2 e le eventuali misure compensative per i rischi residui accettati;
- riceve, con cadenza almeno annuale, una relazione sullo stato di attuazione delle misure di sicurezza informatica e sull'avanzamento del Piano di adeguamento;
- delibera sulle risorse finanziarie e umane necessarie all'attuazione del programma di sicurezza informatica.

Il consiglio di amministrazione può avvalersi del supporto tecnico del responsabile della sicurezza informatica e del comitato per la sicurezza informatica di cui ai paragrafi successivi per l'esercizio delle proprie funzioni in materia.

4.2 Rettore

Il Rettore esercita la responsabilità di indirizzo politico-amministrativo in materia di sicurezza informatica e rappresenta l'ateneo nei confronti delle autorità competenti, inclusa l'Agenzia per la Cybersicurezza Nazionale - ACN e il Ministero dell'Università e della Ricerca - MUR quale autorità NIS di settore. In particolare:
- designa formalmente il punto di contatto NIS e il relativo sostituto, con comunicazione all'ACN;
- può delegare le funzioni operative in materia ICT e sicurezza informatica, con atto formale pubblicato sul sito istituzionale dell'ateneo;
- assicura che la sicurezza informatica sia considerata nella pianificazione strategica e nella programmazione delle risorse dell'ateneo;
- promuove la cultura della sicurezza informatica a tutti i livelli dell'organizzazione.

4.3 **Delegato del rettore per le materie ICT e sicurezza informatica**

Il rettore può nominare, con proprio decreto, un delegato per le materie ICT e sicurezza informatica, scelto preferibilmente tra i professori o ricercatori dell'ateneo con competenze nel settore. Il delegato:
- supporta il rettore e il consiglio di amministrazione nelle decisioni strategiche in materia di sicurezza informatica;
- presiede il comitato per la sicurezza informatica di cui al paragrafo 4.5;
- coordina il raccordo tra gli organi di governance e le strutture operative;
- riferisce periodicamente al rettore e al consiglio di amministrazione sull'andamento del programma di sicurezza informatica.

In assenza di nomina del delegato, le funzioni di cui al presente paragrafo sono esercitate direttamente dal rettore o dal direttore generale per la parte di competenza amministrativa.

4.4 **Direttore generale**

Il direttore generale assicura il raccordo tra gli indirizzi strategici degli organi di governo e la gestione operativa della sicurezza informatica da parte delle strutture amministrative. In particolare:
- garantisce che le misure di sicurezza informatica siano integrate nei processi amministrativi e organizzativi dell'ateneo;
- assicura la disponibilità delle risorse umane e strumentali necessarie all'attuazione del presente regolamento e del Piano di adeguamento NIS 2;
- sovrintende all'attuazione delle decisioni degli organi di governo in materia di sicurezza informatica da parte delle strutture amministrative;
- partecipa, o delega un proprio rappresentante, alle riunioni del comitato per la sicurezza informatica.

4.5 **Comitato per la sicurezza informatica**

È istituito il comitato per la sicurezza informatica (di seguito "il comitato"), organo collegiale con funzioni di coordinamento, indirizzo operativo e raccordo tra le diverse componenti dell'organizzazione per la sicurezza informatica.
Il comitato è composto da:

- il delegato del rettore per le materie ICT e sicurezza informatica, o in sua assenza, il direttore generale, con funzioni di presidente;
- il responsabile IT
- il responsabile della sicurezza informatica
- il data protection officer (DPO);
- il punto di contatto NIS o suo sostituto;
- un rappresentante per ciascuna delle seguenti strutture: area finanza e risorse umane, servizio affari legali e servizio affari istituzionali;

Il comitato può essere estemporaneamente integrato nella sua composizione da eventuali esperti e/o referenti di struttura in ragione degli argomenti trattati.
Il comitato:
- approva le procedure operative in materia di sicurezza informatica;
- monitora l'attuazione del Piano di adeguamento NIS 2 e propone eventuali aggiornamenti;
- esamina i risultati delle attività di valutazione del rischio e propone le priorità di trattamento;
- analizza gli incidenti di sicurezza significativi e definisce le azioni correttive;
- propone al consiglio di amministrazione le misure che richiedono approvazione formale.

Il comitato si riunisce con cadenza almeno semestrale e ogni qualvolta venga convocato dal presidente per ragioni di urgenza, in particolare a seguito di incidenti significativi o mutamenti rilevanti del profilo di rischio. Le riunioni sono verbalizzate e i verbali conservati agli atti dell'ateneo.

4.6 **Responsabile della sicurezza informatica**

Il responsabile della sicurezza informatica è nominato con decreto del rettore, su proposta del direttore generale, e risponde funzionalmente al delegato del rettore per le materie ICT. Costituisce il punto di riferimento operativo per tutte le questioni relative alla cybersecurity dell'ateneo. In assenza di nomina le sue funzioni sono svolte dal responsabile IT.
Il responsabile della sicurezza informatica
- coordina la definizione, l'attuazione e il mantenimento del sistema di gestione della sicurezza informatica dell'ateneo;
- supervisiona l'attuazione del Piano di adeguamento NIS 2 e delle singole azioni di rimedio;
- gestisce il processo di valutazione e trattamento del rischi di natura informatica;
- supervisiona le attività di gestione degli incidenti e coordina la risposta agli eventi di sicurezza significativi;
- predispone le relazioni periodiche per gli organi di governo sull'andamento della sicurezza informatica;
- mantiene aggiornato l'elenco del personale con ruoli e responsabilità in materia di sicurezza informatica;
- coordina le attività di formazione e sensibilizzazione del personale;
- gestisce i rapporti con l'ACN, il CSIRT Italia e il MUR per le questioni di competenza.

4.7 **Responsabile IT**

Il responsabile IT è responsabile della gestione operativa delle infrastrutture tecnologiche dell'ateneo e dell'implementazione tecnica delle misure di sicurezza informatica. In particolare:
- implementa e mantiene le misure tecniche di sicurezza definite nel Piano di adeguamento NIS 2;
- gestisce gli inventari degli asset hardware e software (misura RM.3);
- sovrintende alla gestione delle identità, delle credenziali e dei controlli di accesso (misura RM.6 e RM.7);
- gestisce il processo di patching e aggiornamento dei sistemi;

TORNA ALL'INDICE

- supervisiona il monitoraggio continuo delle reti e dei sistemi (misura RM.10);
- gestisce i backup e le misure di continuità operativa dal punto di vista tecnico (misura BC.2);
- supporta il responsabile della sicurezza informatica nelle attività di valutazione del rischio e gestione degli incidenti.

Le funzioni di responsabile IT sono svolte dal dirigente dell'area tecnica.

4.8 **Punto di contatto NIS e sostituto**

Il punto di contatto NIS è il referente ufficiale dell'ateneo nei confronti dell'ACN e del MUR per gli adempimenti previsti dalla normativa NIS 2. È nominato dal rettore con apposito provvedimento formale, comunicato all'ACN entro i termini di legge, e aggiornato annualmente sulla piattaforma ACN tra l'1 gennaio e il 28 febbraio di ciascun anno. È designato altresì un sostituto che esercita le funzioni del punto di contatto NIS in caso di assenza o impedimento.

Il punto di contatto NIS:

- riceve e trasmette le comunicazioni ufficiali con l'ACN e il MUR;
- coordina gli adempimenti di registrazione e aggiornamento sulla piattaforma ACN;
- garantisce il flusso informativo tra l'ateneo e le autorità competenti in caso di incidenti significativi;
- partecipa alle iniziative e agli aggiornamenti promossi dall'ACN e dal MUR nell'ambito del programma NIS 2.

4.9 **Data protection officer - DPO**

Il data protection officer, già nominato ai sensi del GDPR, collabora con il responsabile della sicurezza informatica per assicurare la coerenza tra le misure di sicurezza informatica e gli obblighi in materia di protezione dei dati personali. In particolare, è coinvolto nella valutazione del rischio per i trattamenti di dati personali, nella gestione degli incidenti con potenziale impatto sui dati degli interessati e nella definizione delle politiche di sicurezza dei dati.

4.10 **Referenti per la sicurezza informatica di struttura**

Per le strutture di maggiore complessità (quali dipartimento, scuola di dottorato, biblioteca, aree dirigenziali ecc.), il responsabile della sicurezza informatica può proporre la designazione di referenti per la sicurezza informatica di struttura, nominati dal direttore generale su proposta dei responsabili delle strutture interessate. I referenti:

- costituiscono il punto di contatto locale per le questioni di sicurezza informatica;
- facilitano la diffusione delle policy e delle procedure operative all'interno della struttura;
- segnalano al responsabile della sicurezza informatica eventuali criticità, anomalie o incidenti rilevati nella struttura di appartenenza;
- partecipano alle attività formative e le promuovono presso il personale della struttura.

Articolo 5

(Elenco del personale con ruoli e responsabilità in materia di cybersecurity)

Il responsabile della sicurezza informatica con il supporto dell'area finanza e risorse umane mantiene e aggiorna un elenco nominativo del personale che riveste ruoli e responsabilità in materia di sicurezza informatica ai sensi del presente regolamento.

L'elenco comprende almeno:

- nominativo e recapiti di contatto;
- ruolo ricoperto ai sensi del presente regolamento;
- struttura di appartenenza;
- data di designazione e, ove applicabile, data di scadenza dell'incarico.

L'elenco è aggiornato entro 30 giorni dal verificarsi di variazioni (nuove nomine, cessazioni, variazioni organizzative) ed è reso disponibile, in forma appropriata, agli Organi di Governo e alle strutture competenti.

TORNA ALL'INDICE

Articolo 6
(Processo di riesame periodico)

Il presente regolamento e l'assetto organizzativo da esso definito sono sottoposti a riesame formale con cadenza almeno biennale, nonché in occasione di:
- incidenti di sicurezza significativi che abbiano evidenziato carenze organizzative;
- variazioni rilevanti nell'assetto organizzativo dell'ateneo;
- mutamenti significativi nel profilo di rischio di natura informatica;
- aggiornamenti normativi che richiedano l'adeguamento dell'organizzazione;
- indicazioni provenienti dall'ACN o dal MUR a seguito di attività di vigilanza.

Il riesame è condotto dal comitato per la sicurezza informatica, che predispone una relazione con le eventuali proposte di modifica, da sottoporre all'approvazione del consiglio di amministrazione.

Articolo 7
(Sanzioni e responsabilità)

Il mancato rispetto degli obblighi previsti dal presente regolamento da parte del personale dell'ateneo può costituire violazione dei doveri d'ufficio, con le conseguenze previste dalla normativa vigente in materia di responsabilità disciplinare dei dipendenti pubblici. Per i collaboratori esterni e i fornitori, le violazioni rilevanti sono gestite nell'ambito dei contratti e degli accordi stipulati con l'ateneo.

Articolo 8
(Comunicazione e diffusione)

Il presente regolamento è:
- pubblicato sul sito istituzionale dell'ateneo
- trasmesso a tutto il personale tecnico-amministrativo e docente
- incluso nei materiali di onboarding per il personale di nuova assunzione e per i collaboratori esterni;
- comunicato all'ACN e al MUR per le parti di competenza.