AMMINISTRAZIONE CENTRALE
AREA SERVIZI INFORMATICI E TELEMATICI
SETTORE SICUREZZA DELLE INFORMAZIONI

UNIVERSITÀ DEGLI STUDI DI PADOVA

Relazione istruttoria per la revisione delle Linee Guida per l'utilizzazione degli strumenti informatici e telematici dell'Università degli Studi di Padova

Revisione 1 del 09/03/2026

Informazioni sul documento

Tipologia e classificazione

Tipo di documento	Classificazione	Distribuzione
BI (Basic Information)	Pubblico	Interna al contesto aziendale

Riferimenti

Codice del documento	Titolo del documento
CP_01	Politica per la sicurezza delle informazioni

Redazione

Azione	Data	Nominativo	Funzione
Redazione	06/03/2026	Settore Sicurezza delle Informazioni	
Verifica	09/03/2026	Giorgio Paolucci	Responsabile SGSI
Approvazione	09/03/2026	Andrea Baraldo	Dirigente IT

Revisioni

Revisione	Data	Descrizione della revisione
1	09/03/2026	Prima stesura

Sommario

1. Premessa

Il presente documento è redatto al fine di avviare formalmente il processo di revisione delle **Linee Guida per l'utilizzazione degli strumenti informatici e telematici dell'Università degli Studi di Padova** approvate con DR il 25 ottobre 2004.

Il periodo trascorso dalla sua approvazione è stato caratterizzato da trasformazioni profonde del contesto tecnologico, organizzativo e normativo entro cui operano le istituzioni universitarie. In particolare, l'infrastruttura digitale degli atenei è progressivamente divenuta una componente essenziale per lo svolgimento delle attività istituzionali di didattica, ricerca e amministrazione, assumendo un ruolo strategico nel funzionamento complessivo delle organizzazioni accademiche.

Parallelamente, il quadro normativo europeo e nazionale relativo alla gestione delle infrastrutture digitali pubbliche, alla protezione dei dati personali e alla sicurezza informatica ha conosciuto negli ultimi anni un significativo rafforzamento.

In tale contesto, appare evidente come il regolamento attualmente vigente, concepito in un contesto tecnologico e normativo ormai profondamente mutato, richieda una revisione complessiva finalizzata a garantirne la piena coerenza con:

- l'attuale quadro normativo europeo e nazionale;
- l'evoluzione delle tecnologie digitali e delle infrastrutture informatiche dell'Ateneo;
- le esigenze operative della comunità universitaria.

Il presente documento ha pertanto lo scopo di illustrare:

- le motivazioni che rendono necessario l'avvio del processo di revisione regolamentare;
- il quadro normativo di riferimento entro cui si colloca tale attività;
- le modalità di lavoro adottate dal gruppo incaricato della predisposizione del piano di revisione;
- gli orientamenti metodologici individuati per lo sviluppo delle attività successive.

2. Evoluzione del contesto tecnologico delle università

Negli ultimi due decenni il sistema universitario ha conosciuto un processo di **progressiva digitalizzazione delle proprie attività**, che ha profondamente modificato le modalità di erogazione dei servizi istituzionali.

Nel periodo in cui fu adottato l'attuale regolamento di Ateneo per l'uso delle risorse informatiche, l'infrastruttura digitale delle università era prevalentemente costituita da reti locali, sistemi di posta elettronica istituzionale e applicativi amministrativi centralizzati. Molte delle tecnologie oggi centrali nel funzionamento delle università non erano ancora diffuse o non avevano assunto la rilevanza attuale.

Nel corso degli ultimi venti anni si è invece assistito a un progressivo ampliamento e a una crescente complessità delle infrastrutture digitali universitarie. Tra i principali fattori di trasformazione possono essere richiamati:

- la diffusione generalizzata della **connettività wireless negli spazi universitari**;
- l'introduzione di piattaforme digitali per la **didattica online e la formazione a distanza**;
- l'adozione di architetture di **cloud computing** e servizi digitali distribuiti;
- la crescente integrazione tra sistemi informativi amministrativi e banche dati istituzionali;
- l'utilizzo sistematico di **identità digitali istituzionali** per l'accesso ai servizi informatici;
- la presenza diffusa di dispositivi personali connessi alle reti universitarie (fenomeno noto come **BYOD – Bring Your Own Device** e ora anche **BYOAI – Bring Your Own AI**).

A tali trasformazioni si aggiunge la crescente diffusione di strumenti basati su **intelligenza artificiale**, sistemi avanzati di analisi dei dati e infrastrutture digitali complesse che supportano attività di ricerca, gestione dei dati scientifici e processi amministrativi automatizzati.

Il crescente grado di integrazione tra infrastrutture digitali e attività istituzionali comporta che eventuali vulnerabilità dei sistemi informativi possano avere ripercussioni significative sul funzionamento complessivo dell'Ateneo.

Per tale ragione, le infrastrutture informatiche universitarie sono oggi considerate parte integrante del patrimonio strategico delle istituzioni accademiche e richiedono forme di governance e regolazione adeguate alla loro rilevanza.

3. Evoluzione del quadro normativo europeo e nazionale

Accanto alle trasformazioni tecnologiche, negli ultimi anni si è registrato un significativo rafforzamento del quadro normativo relativo alla gestione delle infrastrutture digitali pubbliche e alla sicurezza dei sistemi informativi.

3.1 Protezione dei dati personali

Uno dei principali interventi normativi in materia è rappresentato dall'adozione del **Regolamento (UE) 2016/679 (General Data Protection Regulation – GDPR)**, che ha profondamente innovato la disciplina europea in materia di protezione dei dati personali.

Il GDPR ha introdotto un sistema di responsabilizzazione ("accountability") dei titolari del trattamento e ha rafforzato gli obblighi relativi alla sicurezza dei dati, alla gestione dei trattamenti effettuati mediante sistemi informatici e alla protezione delle informazioni personali.

Nel contesto universitario, tali disposizioni assumono particolare rilievo in considerazione dell'elevato volume di dati personali trattati attraverso i sistemi informativi istituzionali, riguardanti studenti, personale, collaboratori e utenti dei servizi digitali.

3.2 Codice dell'amministrazione digitale

Un ulteriore pilastro del quadro normativo nazionale è rappresentato dal **decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale – CAD)**, che disciplina l'utilizzo delle tecnologie dell'informazione e della comunicazione nell'attività delle pubbliche amministrazioni.

Il CAD stabilisce principi fondamentali relativi:

- alla digitalizzazione dei procedimenti amministrativi;
- alla gestione dei documenti informatici;
- alla sicurezza delle infrastrutture digitali pubbliche;
- all'interoperabilità dei sistemi informativi delle pubbliche amministrazioni.

Le disposizioni del CAD sono integrate dalle **linee guida emanate dall'Agenzia per l'Italia Digitale (AgID)**, che definiscono standard tecnici e organizzativi per la gestione delle infrastrutture digitali pubbliche.

3.3 Sicurezza informatica e cybersicurezza nazionale

Negli ultimi anni il tema della sicurezza informatica ha assunto una crescente rilevanza anche nel contesto della sicurezza nazionale.

Con il **decreto-legge 21 settembre 2019, n. 105**, convertito nella legge 18 novembre 2019, n. 133, è stato istituito il **Perimetro di sicurezza nazionale cibernetica**, volto a garantire la protezione delle infrastrutture digitali strategiche per il Paese.

Successivamente, con il **decreto-legge 14 giugno 2021, n. 82**, è stata istituita l'**Agenzia per la Cybersicurezza Nazionale (ACN)**, alla quale sono state attribuite funzioni di coordinamento e indirizzo delle politiche nazionali di cybersicurezza.

L'ACN emana linee guida, raccomandazioni e standard tecnici finalizzati a rafforzare la sicurezza delle infrastrutture digitali pubbliche e private considerate rilevanti per il sistema Paese.

A livello europeo, analoghe attività di indirizzo tecnico sono svolte dall'**ENISA (European Union Agency for Cybersecurity)**, che promuove standard e buone pratiche in materia di sicurezza delle reti e dei sistemi informativi.

4. La direttiva NIS2 e i suoi effetti sulle università

Particolare rilievo assume, nel quadro normativo europeo, la recente adozione della **Direttiva (UE) 2022/2555**, nota come **direttiva NIS2**.

La direttiva NIS2 sostituisce e rafforza la precedente direttiva NIS del 2016, introducendo un sistema più articolato di obblighi finalizzati a garantire un elevato livello comune di sicurezza delle reti e dei sistemi informativi nei settori ritenuti critici per il funzionamento delle società europee.

La normativa distingue tra:

1. **entità essenziali**
2. **entità importanti**

soggette a differenti livelli di vigilanza e obblighi organizzativi.

Tra gli adempimenti previsti dalla direttiva figurano:

1. l'adozione di **politiche di gestione del rischio informatico**;
2. la definizione di procedure per la **gestione degli incidenti di sicurezza**;
3. l'implementazione di misure tecniche e organizzative adeguate alla protezione delle infrastrutture digitali;
4. la predisposizione di sistemi di governance della sicurezza informatica.

Le università di grandi dimensioni, tra cui l'Università degli Studi di Padova, sono stati classificati come **entità essenziali** ai sensi della normativa europea, con conseguente applicazione degli obblighi sopra richiamati.

L'adeguamento alla normativa NIS2 richiede l'adozione di una serie articolata di policy e documenti organizzativi relativi alla sicurezza delle infrastrutture informatiche.

Una prima ricognizione di tali documenti è riportata nella **tabella contenuta nell'Allegato 2** al presente documento.

5. Costituzione del gruppo di lavoro

Alla luce delle considerazioni sopra esposte, l'ASIT (in qualità di amministrazione competente) ha ritenuto opportuno avviare un processo strutturato di revisione del regolamento per l'uso delle risorse informatiche.

A tal fine è stato istituito uno **specifico gruppo di lavoro interdisciplinare**, composto prevalentemente da personale interno all'Ateneo.

Il gruppo riunisce competenze provenienti da diversi ambiti, tra cui:

1. gestione delle infrastrutture informatiche;
2. sicurezza delle reti e dei sistemi informativi;
3. diritto dell'informatica e protezione dei dati personali;
4. organizzazione e gestione amministrativa.

La scelta di valorizzare principalmente competenze interne risponde all'esigenza di fondare il processo di revisione su una conoscenza diretta delle infrastrutture digitali e delle prassi operative dell'Ateneo.

6. Ricognizione della prassi interna

Una prima fase delle attività del gruppo di lavoro è stata dedicata alla **ricognizione delle prassi operative attualmente in uso nell'Ateneo**.

Nel corso degli anni, l'evoluzione tecnologica ha portato allo sviluppo di numerose procedure operative e linee guida tecniche che regolano l'utilizzo delle infrastrutture informatiche.

Tali prassi riguardano, tra l'altro:

1. la gestione delle credenziali di accesso ai servizi digitali;
2. l'utilizzo delle infrastrutture di rete;
3. la gestione dei dispositivi connessi alle reti istituzionali;
4. la sicurezza dei sistemi informativi;
5. la gestione degli incidenti informatici.

In molti casi tali procedure si sono consolidate nel tempo senza trovare un'esplicita formalizzazione nel regolamento vigente.

7. Analisi comparata dei regolamenti di altri atenei

Parallelamente alla ricognizione interna, il gruppo di lavoro ha condotto una **analisi comparata dei regolamenti adottati da altri atenei italiani**.

Sono stati esaminati regolamenti adottati da un campione di università italiane, con particolare attenzione ad alcuni **mega atenei** (come Padova) individuati nella classificazione elaborata dal **CENSIS**.

Il confronto ha consentito di individuare una pluralità di approcci regolamentari e di soluzioni organizzative, lasciando altresì emergere come **molti mega atenei non abbiano di fatto alcun regolamento (pubblico)** che vada oltre la gestione della privacy.

L'analisi, pur parziale, ha evidenziato una **significativa eterogeneità nei modelli regolamentari adottati**, sia con riferimento alla struttura dei documenti sia con riferimento ai contenuti disciplinati.

I risultati di tale analisi sono sintetizzati nella **tavola comparativa riportata nell'Allegato 1**.

8. Coordinamento tra regolamenti e policy di sicurezza

L'analisi svolta dal gruppo di lavoro ha evidenziato come l'introduzione degli obblighi derivanti dalla direttiva NIS2 comporti la necessità di adottare numerose policy interne in materia di sicurezza informatica.

Tali policy riguardano, tra l'altro:

1. la gestione del rischio informatico;
2. la sicurezza delle infrastrutture di rete;
3. la gestione delle vulnerabilità;
4. la gestione degli incidenti di sicurezza;
5. la continuità operativa e il disaster recovery.

Molte di queste materie sono tradizionalmente disciplinate anche nei regolamenti relativi all'uso delle risorse informatiche.

Di conseguenza, vi è il rischio che la produzione di nuovi documenti richiesti dalla normativa NIS2 possa determinare **sovrapposizioni o incoerenze nel quadro regolamentare interno**.

9. Orientamenti metodologici del gruppo di lavoro

Alla luce delle considerazioni sopra esposte, il gruppo di lavoro ha ritenuto opportuno adottare un approccio metodologico articolato.

In particolare, si è ritenuto di **attribuire priorità al processo di adeguamento dell'Ateneo agli obblighi derivanti dalla direttiva NIS2**, procedendo in primo luogo all'adozione delle policy richieste dalla normativa europea.

Successivamente sarà possibile valutare:

1. l'opportunità di aggiornare il regolamento vigente;
2. la possibilità di integrare il regolamento con le nuove policy di sicurezza;
3. oppure la convenienza di procedere alla redazione di un nuovo regolamento organico.

10. Conclusioni

Il processo di revisione del regolamento per l'uso delle risorse informatiche si inserisce in un contesto caratterizzato da profonde trasformazioni tecnologiche e normative.

Rispetto al contesto nel quale fu adottato il regolamento vigente, oggi assumono rilievo tematiche quali:

1. cloud computing;
2. intelligenza artificiale;
3. cybersecurity;
4. gestione dei dispositivi personali connessi alle reti istituzionali;
5. protezione delle infrastrutture digitali critiche.

Il lavoro avviato dal gruppo di lavoro costituisce pertanto il primo passo verso la definizione di un sistema regolamentare aggiornato e coerente con il quadro normativo vigente.

ALLEGATO 1
Ricognizione comparativa di alcuni regolamenti universitari sull'utilizzo delle risorse informatiche

Il presente allegato riporta una ricognizione comparativa dei principali regolamenti adottati da alcuni Atenei italiani in materia di utilizzo delle risorse informatiche, al fine di evidenziare differenze di impostazione, contenuto e livello di dettaglio.

1. Tavola sinottica dei regolamenti analizzati

Ateneo	Aggiornamento	Estensione	Struttura	Principali contenuti	Livello di dettaglio
Padova	2004	~14 pp	Linee guida	Uso risorse, utenti, incidenti informatici, sicurezza di base	Medio
Ferrara	2025	~40 pp	Regolamento articolato	Credenziali, cloud, log, incidenti, dotazioni ICT	Alto
Verona	2022	23 pp	Linee guida operative	Password, antivirus, BYOD, cloud, email	Alto
Bari	2017	11 pp	Regolamento sintetico	Uso corretto risorse e responsabilità utenti	Medio-basso
Genova	2024	19 pp	Linee guida ICT	Sicurezza informatica, dispositivi, cloud	Medio-alto
Pavia	2023	25 pp	Regolamento privacy + ICT	Privacy, sicurezza dati, identità digitali	Alto
Bologna	2009/2013	50+ pp	Testo unico	Privacy, rete, incident response, credenziali	Molto alto
Pisa	2025	10 pp	Linee guida operative	Assegnazione risorse e gestioneidentità	Basso

2. Copertura tematica dei regolamenti

Ateneo	Cloud	BYOD	Incident response	Governance sicurezza	Gestione rischio ICT

Padova	No	No	Sì	No	No
Ferrara	Sì	Parziale	Sì	Parziale	No
Verona	Sì	Sì	Parziale	No	No
Bari	No	No	No	No	No
Genova	Sì	Sì	Parziale	Parziale	No
Pavia	Sì	Parziale	Sì	Parziale	No
Bologna	No	No	Sì	Parziale	No
Pisa	No	No	No	No	No

3. Cronologia dei regolamenti analizzati

Anno	Ateneo	Tipo documento
2004	Università di Padova	Linee guida utilizzo risorse informatiche
2009/2013	Università di Bologna	Testo unico privacy e sistemi informativi
2017	Università di Bari	Regolamento utilizzo risorse informatiche
2022	Università di Verona	Linee guida uso strumenti informatici
2023	Università di Pavia	Regolamento privacy e risorse informatiche
2024	Università di Genova	Linee guida sicurezza ICT
2025	Università di Ferrara	Regolamento uso risorse informatiche
2025	Università di Pisa	Linee guida assegnazione risorse ICT

Osservazione generale: l'analisi evidenzia una significativa eterogeneità nei regolamenti degli Atenei italiani sia per quanto riguarda l'estensione sia per quanto riguarda i contenuti disciplinati. In particolare, solo alcuni regolamenti recenti includono temi quali cloud computing, BYOD e gestione degli incidenti informatici.

ALLEGATO 2
Ricognizione obblighi NIS2 e D.Lgs. 138/2024
Confronto con Linee Guida UNIPD 2004

Tavola sinottica con classificazione semaforica

Legenda:
- tema già dettagliatamente affrontato
- tema marginalmente affrontato
- tema non affrontato

Ambito	Riferimento normative	Contenuto dell'obbligo	Stato nel regolamento UNIPD 2004	Osservazioni
Governance della cybersicurezza	Art. 20 Dir. NIS2; art. 23 D.Lgs. 138/2024	Responsabilità degli organi di vertice sulla sicurezza	Tema non affrontato	Assente disciplina sulla governance della sicurezza
Gestione del	Art. 21 Dir.	Sistema di	Tema non	Il regolamento

rischio	NIS2; art. 24 D.Lgs. 138/2024	gestione del rischio cyber	affrontato	non prevede metodologie di risk management
Politiche di sicurezza	Art. 21 Dir. NIS2; art. 24 D.Lgs. 138/2024	Policy formalizzate di sicurezza	Tema marginalmente affrontato	Art. 25 prevede alcune misure di sicurezza ma non sistemiche
Gestione incidenti	Art. 21 Dir. NIS2; artt. 25- 27 D.Lgs. 138/2024	Procedure di gestione incidenti	Tema già dettagliatamente affrontato	Definizione di incidente e procedura dettagliata
Notifica incidenti	Art. 23 Dir. NIS2; artt. 25- 27 D.Lgs. 138/2024	Notifica incidenti all'autorità competente	Tema non affrontato	Il regolamento prevede solo comunicazioni interne
Continuità operative	Art. 21 Dir. NIS2	Business continuity e disaster recovery	Tema non affrontato	Assente qualsiasi riferimento alla continuità operativa
Supply chain ICT	Art. 21 Dir. NIS2	Gestione rischio fornitori ICT	Tema non affrontato	Il regolamento non tratta servizi esternalizzati
Gestione accessi	Art. 21 Dir. NIS2	Controllo accessi ai sistemi	Tema marginalmente affrontato	Artt. 17- 18 prevedono requisiti di accesso alle risorse
Software e licenze	Normativa copyright	Uso legittimo del software	Tema già dettagliatamente affrontato	Esplicito obbligo di software regolarmente licenziato
Protezione malware	Art. 21 Dir. NIS2	Misure contro programmi malevoli	Tema già affrontato	Art. 25 prevede strumenti di protezione

Monitoraggio risorse	Art. 24 D.Lgs. 138/2024	Monitoraggio e logging attività	Tema già affrontato	Previsti monitoraggi delle risorse e controlli
Regime sanzionatorio	Normativa disciplinare	Sistema sanzionatorio per uso improprio	Tema già dettagliatamente affrontato	Presente schema delle sanzioni

Nota metodologica: la classificazione evidenzia che le Linee Guida del 2004 disciplinano principalmente l'uso delle risorse informatiche e le responsabilità degli utenti, mentre non affrontano in modo sistemico gli aspetti di governance della cybersicurezza richiesti dalla Direttiva NIS2 e dal D.Lgs. 138/2024.