Regolamento delle risorse e dei servizi informatici del Dipartimento di Ingegneria Industriale

Premessa

Il presente regolamento ha la finalità di definire in modo organico le modalità di utilizzo consentite e non consentite delle risorse informatiche, al fine di garantire la sicurezza, la continuità operativa dei servizi e la tutela dei dati, in conformità al Regolamento generale sulla protezione dei dati (GDPR – Regolamento (UE) 2016/679), al D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, e alle disposizioni applicabili della Direttiva europea (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recepita nell'ordinamento italiano con il D.Lgs. 138/2024.

La rete informatica del Dipartimento è l'insieme delle infrastrutture e degli apparati che consentono la connessione dei dispositivi e l'accesso ai servizi informatici e a Internet. Essa costituisce uno strumento di lavoro essenziale a supporto della didattica, della ricerca, della terza missione e delle attività amministrative.

Art. 1 - Risorse informatiche e ambito di applicazione

Le risorse informatiche messe a disposizione dall'Ateneo o dal Dipartimento costituiscono un patrimonio comune e uno strumento di lavoro essenziale a supporto della didattica, della ricerca, della terza missione e delle attività amministrative. Esse comprendono, a titolo esemplificativo e non esaustivo:

- la rete informatica dipartimentale, costituita dalle infrastrutture e dagli apparati che consentono la connessione cablata e wireless dei dispositivi e l'accesso ai servizi informatici e a Internet;
- i server e i sistemi di archiviazione;
- i servizi di autenticazione e di gestione delle identità digitali;
- le postazioni di lavoro e i dispositivi mobili;
- i servizi cloud e le piattaforme digitali istituzionali;
- i software e le applicazioni.

Tali risorse sono organizzate e gestite per assicurare la disponibilità, l'integrità e la riservatezza delle informazioni trattate, nonché la tracciabilità delle operazioni nei limiti e secondo le modalità previste dalla normativa applicabile e dalle disposizioni dell'Università degli Studi di Padova.

Il presente regolamento si applica a tutti coloro che, a qualsiasi titolo, utilizzano le risorse informatiche del Dipartimento, ovvero docenti, ricercatori, personale tecnico-amministrativo, incarichi di ricerca, dottorandi, studenti, borsisti, collaboratori, docenti e ricercatori ospiti e altri soggetti autorizzati dal

Regolamento Accessi. Si applica altresì all'utilizzo di dispositivi personali limitatamente alla loro connessione alla rete dipartimentale e all'accesso alle risorse e ai servizi informatici del Dipartimento.

Art. 2 - Utilizzo delle risorse informatiche e attività consentite

Le risorse informatiche del Dipartimento sono destinate principalmente allo svolgimento delle attività istituzionali di didattica, ricerca, terza missione e amministrazione.

È consentito, nel rispetto delle autorizzazioni attribuite a ciascun utente:

- navigare su Internet per attività di studio, ricerca e lavoro;
- utilizzare software regolarmente licenziato e autorizzato;
- accedere ai servizi e alle piattaforme istituzionali, quali posta elettronica, piattaforme didattiche e repository;
- utilizzare strumenti digitali per la gestione amministrativa e la collaborazione scientifica e accademica;
- trasferire e condividere dati mediante strumenti e protocolli sicuri, quali HTTPS e VPN autorizzate, nel rispetto dei vincoli di accesso e riservatezza delle informazioni trattate;
- utilizzare servizi cloud approvati dall'Ateneo o dal Dipartimento.

Art. 3 - Collegamento dei dispositivi e requisiti di sicurezza

Possono essere collegati alla rete dipartimentale:

- computer e altri dispositivi acquistati con fondi del Dipartimento o fondi di ricerca;
- dispositivi personali, quali computer portatili e tablet, purché conformi ai requisiti di sicurezza di seguito indicati. Non è invece consentito introdurre e utilizzare nei locali del Dipartimento computer fissi personali e relative periferiche, anche se non collegati alla rete dipartimentale.

Tutti i dispositivi collegati devono:

- utilizzare un sistema operativo supportato e aggiornato, con gli aggiornamenti di sicurezza installati;
- disporre di una protezione antimalware attiva e aggiornata, ove applicabile alla tipologia di dispositivo;
- utilizzare software regolarmente licenziato;
- non presentare segnali di compromissione o generare traffico riconducibile ad attività malevole.

I dispositivi non conformi ai requisiti sono esclusi dalla rete fino al ripristino delle condizioni di sicurezza. Eventuali esigenze connesse a strumentazione scientifica o sistemi particolari sono sottoposte alla valutazione prevista nell'Art.8.

I dispositivi personali, anche se utilizzati per attività lavorative, non sono oggetto di assistenza tecnica da parte del personale informatico del Dipartimento. Resta fermo l'obbligo di segnalare eventuali incidenti che possano coinvolgere la rete o i servizi dipartimentali.

È vietato collegare alla rete dipartimentale apparati quali modem, router, switch e access point senza la preventiva autorizzazione del Settore Servizi Informatici, indipendentemente dalla proprietà o dai fondi utilizzati per l'acquisto.

È inoltre vietato intervenire sui cablaggi di rete o di alimentazione delle infrastrutture e degli apparati condivisi, modificandoli, scollegandoli o manomettendoli. Eventuali interventi devono essere richiesti al Settore Servizi Informatici ed eseguiti dal personale incaricato.

Art. 4 - Utilizzi non consentiti delle risorse informatiche

Per il corretto utilizzo delle risorse informatiche del Dipartimento sono vietate le seguenti attività:

- utilizzare software non autorizzato o non regolarmente licenziato;
- installare programmi provenienti da fonti non affidabili;
- introdurre o diffondere virus, malware o altri contenuti dannosi;
- effettuare scansioni di rete, tentativi di intrusione o accessi a sistemi e dati senza autorizzazione;
- aggirare i sistemi di sicurezza, anche mediante proxy, VPN non autorizzate o servizi di anonimizzazione;
- svolgere attività di mining di criptovalute;
- utilizzare programmi peer-to-peer non autorizzati;
- generare traffico anomalo o eccessivo non giustificato da attività istituzionali;
- attivare servizi o modificare configurazioni di rete senza le necessarie autorizzazioni.

Le suddette attività potranno essere bloccate automaticamente dai sistemi di protezione della rete.

Le esigenze di ricerca che richiedono attività o configurazioni altrimenti non consentite devono essere preventivamente sottoposte alla procedura prevista nell'Art.8.

Art. 5 - Responsabilità degli utenti

Il corretto utilizzo delle risorse informatiche da parte di tutti gli utenti è essenziale per la protezione dell'intera infrastruttura digitale. Comportamenti impropri, anche involontari, possono compromettere la sicurezza dei sistemi e dei dati e pregiudicare la continuità dei servizi.

Ogni utente è tenuto, nell'ambito delle proprie competenze e autorizzazioni, a:

- mantenere aggiornati i dispositivi di cui cura direttamente la gestione e consentire gli interventi di aggiornamento sui dispositivi gestiti dal personale informatico;
- custodire le proprie credenziali e non condividerle con altre persone;
- bloccare la sessione di lavoro quando si allontana dalla postazione;

- prestare attenzione a messaggi, collegamenti e allegati sospetti;
- conservare i dati di lavoro negli spazi istituzionali previsti e assicurarne il backup secondo le indicazioni del Settore Servizi Informatici; l'utilizzo di servizi di sincronizzazione cloud non sostituisce, di per sé, un sistema di backup;
- segnalare tempestivamente anomalie, sospetti incidenti o compromissioni delle credenziali;
- attenersi alle indicazioni del personale informatico per la protezione dei sistemi e il ripristino dei servizi;
- spegnere i dispostivi di Dipartimento al termine dell'utilizzo.

Art. 6 - Monitoraggio e misure di sicurezza

Il traffico di rete e gli eventi di sicurezza possono essere monitorati dal personale autorizzato per individuare e contrastare attacchi informatici, rilevare anomalie e garantire il corretto funzionamento dei servizi.

I controlli sono effettuati per finalità di sicurezza e gestione tecnica, nel rispetto della normativa applicabile in materia di protezione dei dati personali e delle disposizioni di Ateneo.

Qualora un dispositivo presenti segnali di compromissione, partecipi anche inconsapevolmente ad attività malevole o costituisca un rischio per l'infrastruttura, il personale informatico può limitarne o sospenderne l'accesso alla rete fino al ripristino delle condizioni di sicurezza.

Art. 7 - Segnalazione e gestione degli incidenti

In caso di sospetto incidente di sicurezza, ad esempio infezione da malware, accesso non autorizzato o comportamento anomalo del dispositivo, l'utente deve:

- scollegare il dispositivo dalla rete cablata e wireless, ove possibile;
- contattare tempestivamente il Settore Servizi Informatici, descrivendo l'anomalia riscontrata;
- evitare interventi autonomi di ripristino, cancellazioni o altre operazioni che possano aggravare il problema o compromettere l'analisi dell'incidente;
- seguire le istruzioni del personale informatico.

Art. 8 - Servizi a supporto della ricerca ed esigenze particolari

Il Dipartimento mette a disposizione di docenti e ricercatori servizi informatici a supporto della ricerca, tra cui infrastrutture per il calcolo ad alte prestazioni (HPC) e servizi centralizzati gestiti dal Settore Servizi Informatici.

Non è consentito:

- installare o gestire autonomamente server all'interno della server farm dipartimentale;
- attivare sistemi di archiviazione accessibili a utenti non registrati o non autorizzati;

- attivare servizi privi di autorizzazione o di una gestione concordata con il Settore Servizi Informatici che possano compromettere la sicurezza o la stabilità dell'infrastruttura.

Le esigenze di ricerca che richiedono configurazioni particolari, servizi aggiuntivi o deroghe alle modalità ordinarie di utilizzo devono essere motivate e sottoposte preventivamente al Settore Servizi Informatici, che ne valuta la fattibilità tecnica, la sicurezza e la sostenibilità operativa.

Le attività possono essere avviate solo dopo il rilascio dell'autorizzazione e devono svolgersi in ambienti controllati, secondo le modalità e le misure di sicurezza concordate.

Art. 9 – Acquisto di dotazioni hardware e software

L'acquisto di apparecchiature informatiche e licenze software destinate alle attività del Dipartimento, anche mediante fondi di ricerca, deve essere preventivamente concordato con il Settore Servizi Informatici.

Il Settore Servizi Informatici:

- verifica e valida le caratteristiche tecniche delle dotazioni in relazione alle finalità d'uso e alla compatibilità con le infrastrutture esistenti;
- fornisce supporto nella scelta delle soluzioni più idonee, sicure e sostenibili sotto il profilo della gestione e della manutenzione;
- verifica l'eventuale disponibilità di dotazioni, licenze o servizi già messi a disposizione dall'Ateneo o dal Dipartimento;
- cura l'istruttoria della procedura di acquisto, in collaborazione con gli uffici amministrativi competenti e nel rispetto delle procedure di Ateneo e del Codice dei contratti pubblici.

Anche per l'acquisto di apparecchiature dotate di connettività di rete, come le stampanti 3D con connessione wireless, è necessario contattare preventivamente il Settore Servizi Informatici e concordare le modalità di collegamento e utilizzo sulla rete dipartimentale.

Non sono ammessi acquisti per attività istituzionali effettuati autonomamente senza il preventivo coinvolgimento del Settore Servizi Informatici, al fine di evitare incompatibilità tecniche, duplicazioni di spesa e criticità di sicurezza o gestione.

Art. 10 - Licenze software

Principi generali

L'utilizzo di software sui dispositivi e sulle infrastrutture del Dipartimento deve rispettare le condizioni di licenza, gli accordi sottoscritti dall'Ateneo o dal Dipartimento e la normativa vigente in materia di proprietà intellettuale.

Tale obbligo si applica anche al software gratuito e open source, il cui utilizzo resta soggetto alle rispettive condizioni di licenza.

Acquisizione e attivazione

L'acquisto di licenze software avviene secondo quanto previsto nell'Art.9. Anche l'attivazione di abbonamenti, licenze gratuite o versioni di prova per uso istituzionale deve essere concordata con il Settore Servizi Informatici.

Prima dell'acquisizione o dell'installazione, gli utenti sottopongono le proprie esigenze al Settore Servizi Informatici, che verifica, con il supporto degli uffici competenti ove necessario:

- l'eventuale disponibilità di licenze già possedute dall'Ateneo o dal Dipartimento;
- la compatibilità con le infrastrutture informatiche esistenti;
- il rispetto dei requisiti di sicurezza e protezione dei dati;
- le condizioni e le eventuali restrizioni d'uso, con particolare riferimento alle attività didattiche, di ricerca e amministrative;
- la durata della licenza, le condizioni di rinnovo e gli eventuali costi ricorrenti.

Installazione e utilizzo

L'installazione è ammessa solo per software dotato di una licenza valida per l'utilizzo previsto, acquisito da fonti ufficiali o affidabili e autorizzato dal Settore Servizi Informatici.

Sui dispositivi gestiti dal Settore Servizi Informatici, le installazioni sono effettuate dal personale informatico o secondo le modalità da esso indicate.

Sono vietati:

- l'installazione e l'utilizzo di copie prive di una valida licenza;
- l'utilizzo di un numero di installazioni o accessi superiore a quello consentito;
- l'elusione dei meccanismi di attivazione o protezione delle licenze;
- la condivisione non autorizzata di credenziali o chiavi di licenza assegnate individualmente.

Responsabilità degli utenti

Gli utenti sono tenuti a:

- rispettare le condizioni di licenza e le modalità di utilizzo autorizzate;
- conservare e rendere disponibile al Settore Servizi Informatici l'eventuale documentazione di licenza o autorizzazione ricevuta direttamente;
- segnalare tempestivamente esigenze di rinnovo, aggiornamento o acquisizione di nuove licenze;
- concordare eventuali trasferimenti delle licenze ad altri utenti o dispositivi.

Verifiche e gestione delle non conformità

Il personale autorizzato può effettuare verifiche periodiche sulla conformità delle installazioni software presenti sui dispositivi e sulle infrastrutture del Dipartimento, nel rispetto della normativa applicabile e delle disposizioni di Ateneo.

Per i dispositivi personali, le verifiche riguardano i requisiti necessari per l'accesso alla rete e ai servizi dipartimentali, secondo quanto previsto negli Artt. 3 e 6.

In caso di software non autorizzato o utilizzato in violazione delle condizioni di licenza, l'utilizzo deve essere interrotto e il software rimosso oppure regolarizzato secondo le indicazioni del Settore Servizi Informatici. Qualora sussistano rischi per la sicurezza, il dispositivo può essere temporaneamente escluso dalla rete.

Restano ferme le eventuali ulteriori misure previste dai regolamenti di Ateneo.

Art. 11 - Utilizzo di servizi cloud, piattaforme SaaS e sistemi di Intelligenza Artificiale

Per le attività istituzionali devono essere utilizzati servizi cloud e piattaforme digitali messi a disposizione dall'Ateneo o dal Dipartimento oppure formalmente autorizzati. L'utilizzo di ulteriori servizi deve essere preventivamente sottoposto al parere del Settore Servizi Informatici.

L'archiviazione, l'elaborazione e la condivisione delle informazioni devono rispettare la normativa sulla protezione dei dati personali, le disposizioni di Ateneo e gli eventuali vincoli contrattuali o di riservatezza. L'autorizzazione all'utilizzo di un servizio non comporta automaticamente la possibilità di inserirvi qualsiasi tipologia di dato.

È vietato caricare dati personali, informazioni riservate o dati di ricerca soggetti a vincoli su piattaforme non autorizzate per il relativo trattamento.

Le medesime disposizioni si applicano agli strumenti di intelligenza artificiale, il cui utilizzo deve inoltre prevedere la verifica dei contenuti generati da parte dell'utente.

Il Settore Servizi Informatici può limitare o bloccare l'accesso ai servizi che presentino rischi per la sicurezza o risultino incompatibili con le disposizioni applicabili.

Art. 12 - Osservanza del regolamento

Tutti gli utenti sono tenuti a utilizzare le risorse informatiche secondo le finalità e le condizioni previste dal presente regolamento, ad adottare comportamenti che tutelino la sicurezza dei sistemi e dei dati e a collaborare con il Settore Servizi Informatici nella prevenzione e nella gestione degli incidenti.

Padova, 27 ottobre 2026

Il Direttore

Fabrizio Dughiero

firmato digitalmente ai sensi del d.lgs. 82/2005

Firmato digitalmente da:
Dughiero Fabrizio
Firmato il 27/10/2026 11:26
Seriale Certificato: 5399717
Valido dal 14/01/2026 al 14/01/2029
InfoCamere Qualified Electronic Signature CA