Università degli Studi di Ferrara

REGOLAMENTO D'USO DELLE RISORSE INFORMATICHE

Emanato con Decreto Rettorale Rep. 10/2025 Prot. n. 2240 del 8/01/2025
Entrata in vigore: 23 gennaio 2025

Sommario

Articolo 1 - Definizioni

1) Al fine del seguente regolamento si premettono le seguenti definizioni:
   a) Sistema informativo: il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate alla acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni;
   b) RTD o suo delegato: il Responsabile per la transizione digitale, come definito dall'art.17 del D.Lgs 7 marzo 2005 n.82 e ss.mm.ii. o la persona da lui delegata per il particolare servizio o ambito, e i cui riferimenti sono pubblicati sul portale di Ateneo;
   c) referenti dei Servizi IT dell'Ateneo: persone, unità o strutture che per delega, incarico o posizione organizzativa hanno specifica responsabilità per il particolare servizio o ambito ICT come desumibile dalle indicazioni di accesso ai servizi pubblicate sul portale di Ateneo;
   d) utenti: tutti coloro che, a diverso titolo, accedono alla rete ed alle risorse informatiche di Ateneo, tra cui docenti e ricercatori, personale tecnico amministrativo, studenti, dottorandi, specializzandi, collaboratori a vario titolo e tutti coloro i quali sono in possesso di credenziali che consentano l'accesso alle risorse informatiche messe a disposizione dall'Ateneo;
   e) utenti strutturati: utenze assegnate a persone giuridicamente inquadrate come personale strutturato.
2) Ulteriori definizioni utili alla piena comprensione del presente regolamento sono contenute nel

glossario in calce allo stesso.

Articolo 2 - Oggetto e finalità

1) Il presente regolamento descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo dell'Università di Ferrara di seguito denominato "Università".

2) Il regolamento ha la finalità di garantire la disponibilità dei servizi, ottimizzare l'impiego delle risorse, introdurre regole per il loro corretto utilizzo nel contesto organizzativo dell'Università e ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati e delle informazioni, nonché di accesso non autorizzato o di trattamento non consentito degli stessi.
3) Il presente regolamento definisce inoltre le modalità di accesso, utilizzo e gestione dei servizi cloud per la produttività (ad esempio, e-mail, calendari, condivisione di file, ecc.) messi a disposizione dall'Ateneo alla comunità universitaria.
4) Tutte le cariche, professioni e titoli inerenti a funzioni nominate nel presente regolamento e declinate al genere maschile devono intendersi riferite anche al corrispondente termine di genere femminile.

Articolo 3 - Ambito di applicazione

1) Il presente regolamento si applica a tutti gli utenti delle risorse informatiche dell'Università, così come definiti nell'Articolo 1.
2) L'uso delle risorse e dei servizi del sistema informativo dell'Università è subordinato al rispetto da parte degli utenti del presente regolamento, oltre che delle norme civili, penali e amministrative applicabili. Le norme che regolano la Rete GARR (Acceptable Use Policy - AUP), la cui versione aggiornata è disponibile sul portale Web del Consortium GARR, costituiscono parte integrante del regolamento nel loro ambito di applicazione.

Articolo 4 - Dotazioni informatiche individuali

1) In relazione al rapporto di lavoro instaurato e alle mansioni affidate, l'Università può assegnare agli utenti una postazione di lavoro per l'accesso alla rete e ai servizi del sistema informativo, un insieme di dotazioni hardware e software individuali, un insieme di risorse e applicativi accessibili in cloud e servizi di stampa, fotocopie e scanner con configurazione predisposta per assicurare la protezione dei dati personali e la riservatezza delle informazioni trattate.

4.1 Postazioni di lavoro dell'Amministrazione centrale

1) Le postazioni di lavoro dell'Amministrazione centrale sono configurate e gestite centralmente dai referenti dei Servizi IT dell'Ateneo nel rispetto del principio di standardizzazione delle postazioni lavorative.

La tipologia e le caratteristiche delle postazioni di lavoro tengono conto delle esigenze lavorative rilevate per gruppi di utenti omogenei, dell'evoluzione tecnologica e del rapporto qualità/prezzo/efficienza delle tecnologie disponibili.

2) Le postazioni di lavoro hanno caratteristiche minime comuni costituite da:
   a) un sistema operativo aggiornato e sicuro;
   b) un antivirus locale con aggiornamento automatico;
   c) una dotazione di applicativi individuali di base omogenei e standardizzati;
   d) la possibilità di accesso da parte di Amministratori di Sistema per l'erogazione dei servizi di assistenza remota e aggiornamento automatico;
   e) la possibilità di configurare parametri standardizzati ai fini di garantire la sicurezza della postazione stessa.
3) Le postazioni di lavoro devono obbligatoriamente essere protette, in caso di assenza anche temporanea, tramite la sospensione o il blocco della sessione di lavoro. A tale fine è impostata automaticamente, da parte degli Amministratori di Sistema responsabili, l'attivazione del blocco dello schermo in un periodo di tempo congruo al fine di impedire la lettura e/o la modifica dei dati presenti a video.
4) Gli utenti possono avanzare richiesta di installazione di software non in dotazione ai referenti dei Servizi IT di Ateneo che ne valutano il rispetto dei requisiti di sicurezza, economicità e idoneità funzionale, sentito il responsabile della struttura di afferenza dell'utente.
5) Il referente del servizio IT di Ateneo competente può inoltre autorizzare singoli utenti, qualora si renda necessario, in seguito a richiesta motivata dell'utente, sulla base di specifiche necessità lavorative, e dopo averne valutato l'adeguatezza delle competenze tecniche necessarie, ad avere privilegi di amministratore della propria postazione di lavoro.

4.2 Postazioni di lavoro delle Strutture decentrate

1) In considerazione delle specifiche esigenze di ricerca e di didattica, le strutture decentrate possono provvedere all'acquisto ed all'assegnazione di dotazioni informatiche ai propri afferenti, selezionandole in base alle specifiche necessità degli assegnatari.
2) Le suddette strutture, se dotate di Amministratori di Sistema competenti nella gestione degli strumenti di standardizzazione, possono richiedere al referente del Servizio IT competente il

decentramento, totale o parziale, delle funzioni di configurazione e gestione delle postazioni di lavoro, che devono comunque essere esercitate nel rispetto del presente regolamento.

3) Sempre considerando le specificità del ruolo e delle necessità dell'utente, il responsabile della struttura, con il supporto dell'Amministratore di Sistema competente, può individuare una dotazione minima di software che debba essere installato e determinare le modalità di gestione e monitoraggio delle postazioni, autorizzare software specifico necessario all'attività di didattica o di ricerca oppure autorizzare l'utilizzatore ad avere accesso amministrativo alla sua postazione di lavoro.
4) L'installazione di ulteriori prodotti e/o pacchetti software, su richiesta motivata di singoli utenti o gruppi, è ammessa previa verifica dei requisiti di sicurezza, economicità e idoneità funzionale degli stessi da parte dell'Amministratore di Sistema competente o, dove non sia nominato, dai referenti dei Servizi IT di Ateneo.

4.3 Postazioni di lavoro in laboratori, biblioteche e spazi comuni

1) Le postazioni di lavoro situate in ambienti ad uso comune, come laboratori didattici, biblioteche e altre aree condivise, sono soggette a regole specifiche che garantiscono la protezione dei dati e la sicurezza informatica, in conformità con il D.lgs. 82/2005 (Codice dell'amministrazione digitale) e le sue successive modifiche.
2) Gli Amministratori di Sistema, in collaborazione con i referenti dei Servizi IT di Ateneo, sono tenuti a:
    a) prevenire la condivisione non autorizzata, accidentale o intenzionale, di dati personali e sensibili attraverso misure che garantiscano la riservatezza dei dati in conformità alle disposizioni del Codice dell'amministrazione digitale, implementando protocolli di protezione adeguati;
    b) assicurare la disponibilità e l'integrità dei sistemi informatici, proteggendo le postazioni da malware, attacchi informatici e uso improprio, attraverso l'utilizzo di software aggiornati e protocolli di sicurezza standardizzati, come previsto dal D.lgs. 82/2005. Le postazioni dovranno essere configurate per prevenire accessi non autorizzati e per garantire che ogni utente possa accedere solo alle risorse per cui è abilitato;

c) monitorare l'uso delle postazioni, garantendo l'identificazione chiara degli utilizzatori, come richiesto dalle normative in materia di tracciabilità e sicurezza delle operazioni digitali, al fine di consentire l'individuazione di eventuali responsabilità in caso di violazioni di sicurezza o richieste dell'autorità giudiziaria.

3) Inoltre, gli Amministratori di Sistema devono garantire che ogni postazione sia configurata in modo da rispettare i principi di accessibilità digitale, assicurando che le tecnologie utilizzate siano compatibili con le linee guida di interoperabilità e usabilità del Codice dell'amministrazione digitale.

4.4 Fotocopia e scanner

1) Gli utenti possono accedere alle stampanti/copiatrici multifunzione messe loro a disposizione delle rispettive strutture di appartenenza, rispettando i principi di utilizzo ragionevole e cercando di limitare le operazioni di stampa allo stretto necessario, secondo criteri di economicità e sostenibilità ambientale.
2) L'Università si riserva la facoltà di monitorare l'utilizzo del servizio, demandando questo compito ai referenti dei Servizi IT dell'Ateneo.

4.5 Corretto utilizzo e conservazione delle dotazioni informatiche di lavoro

1) Le dotazioni informatiche di lavoro, insieme agli accessori fisici e alle dotazioni software individuali, devono essere:
   a) consegnate ad ogni nuovo utente, nei limiti delle sue necessità e coerentemente con il suo inquadramento giuridico, con la configurazione standard di base aggiornata alla data di consegna;
   b) utilizzate e conservate con diligenza al fine di ottimizzare l'impiego delle risorse dell'Università, il risparmio energetico e l'impatto ambientale, nel rispetto del presente regolamento e del Codice di comportamento dei dipendenti dell'Università;
   c) utilizzate in modo pertinente alle specifiche finalità dell'Università, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
   d) custodite, anche in caso di trasferimento di sede e struttura dell'utente, insieme a tutte le altre dotazioni strumentali personali;
   e) restituite immediatamente in caso di cessazione del rapporto di lavoro e/o collaborazione.

2) I file contenenti dati personali o informazioni riservate devono essere salvati utilizzandolo spazio di archiviazione remoto (file server o cloud) messo a disposizione dell'Università, avendo cura di eliminare file obsoleti o non più necessari e nel rispetto della quota di risorse assegnata. In caso di sostituzione o guasto della postazione di lavoro, l'assistenza utenti non effettua operazioni di ripristino di dati e informazioni salvati sui dischi locali della postazione.
3) È possibile derogare al salvataggio dei dati nello spazio di archiviazione remoto messo a disposizione dell'Università, di cui al paragrafo precedente, nel caso questo sia espressamente vietato da accordi specifici (ad es. accordi di ricerca che lo prevedano espressamente) o da considerazioni di opportunità adeguatamente motivate, fermo restando la necessità di garantire un livello di protezione almeno pari a quello offerto dai servizi forniti dall'Ateneo e il rispetto di tutte le norme previste dal presente regolamento e dalla normativa in materia.
4) Le dotazioni restituite, ritirate per riparazione o sostituite per aggiornamento della dotazione, vengono riconfigurate dagli Amministratori di Sistema competenti in modo da cancellare in modo sicuro ogni dato preesistente e riportate alla configurazione standard del momento. Le dotazioni riconfigurate vengono consegnate al magazzino delle dotazioni disponibili per altri utenti.

4.6 Assistenza e interventi sulle postazioni di lavoro

1) Gli Amministratori di Sistema formalmente designati possono, sulle postazioni sulle quali è prevista l'installazione di apposito software, collegarsi in modalità remota alla postazione di lavoro, allo scopo di assicurare l'assistenza tecnica, la sicurezza e l'operatività, effettuando operazioni di manutenzione e aggiornamento del software installato. Gli interventi sono effettuati dagli Amministratori di Sistema accedendo alla postazione con proprie credenziali e privilegi di Amministratore.
2) Nei casi in cui l'utente segnali malfunzionamenti per la soluzione dei quali, a scopi diagnostici, sia indispensabile impersonare l'utente e accedere con i privilegi allo stesso assegnati, l'intervento viene effettuato solo su specifica richiesta e autorizzazione dell'utente stesso.
3) In mancanza di autorizzazione dell'utente, o nel caso in cui l'utente sia amministratore della propria postazione e non conceda accesso amministrativo al personale incaricato, non è garantita l'assistenza tecnica.

4) Tutte le operazioni di collegamento remoto vengono tracciate dai sistemi informatici che registrano, in maniera non alterabile, le informazioni relative all'intervento effettuato.

Articolo 5 - Utilizzo di postazioni di lavoro portatili

1) Se la dotazione fornita dall'Università prevede l'utilizzo di computer portatili, l'assegnatario della risorsa deve adottare comportamenti adeguati a prevenire l'accesso da parte di soggetti non autorizzati in ragione della:
   a) natura dei dispositivi: tali dispositivi sono facilmente trasportabili ed occultabili;
   b) natura dei dati presenti sui dispositivi mobili: possono essere presenti copie parziali e/o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;
   c) modalità di utilizzo dei dispositivi: possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Università ed in aree non sicure e ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui ci si riconnette alla rete interna.

5.1 Prevenzione

1) Per quanto sopra precisato è fatto divieto ad ogni utente di salvare in locale credenziali senza adeguate protezioni (es. cifratura) che consentano l'accesso alla rete o ad applicazioni dell'Università.
2) Al fine di evitare accessi non autorizzati ai dati e ai servizi dell'Università gli utilizzatori sono tenuti a:
   a) memorizzare in forma protetta i file che contengono categorie particolari di dati, così come definiti dall'art. 9 del regolamento UE 679/2016, o dati giudiziari (a titolo esemplificativo e non esaustivo: proteggere l'accesso a cartelle o file tramite password, o all'intero supporto di memorizzazione, utilizzando appositi strumenti di cifratura);
   b) quando non più necessari, distruggere i supporti rimovibili contenenti dati di particolari categorie e/o relativi a condanne penali e reati, o rendere inintelligibili i dati in essi contenuti.
3) Per prevenire furto, danneggiamento involontario e comunque situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, l'utente è tenuto a:

a) custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio, ecc.);
b) durante il trasporto osservare le istruzioni del fabbricante per la protezione dei dispositivi da urti, campi elettromagnetici e sbalzi di temperatura;
c) trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
d) non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;
e) non lasciare i dispositivi in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno;
f) non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.

4) I computer portatili ad uso individuale devono essere utilizzati esclusivamente dall'utente a cui gli stessi sono stati assegnati e, qualora siano assegnati alle strutture, il loro utilizzo deve essere regolamentato dalle stesse, in funzione delle proprie peculiarità ed in modo tale da garantirne il controllo.
5) Gli utenti assegnatari provvedono al collegamento delle postazioni di lavoro portatili alla rete dell'Università anche attraverso l'uso della VPN messa a disposizione dall'Ateneo, almeno una volta ogni 30 giorni, per effettuare gli aggiornamenti automatici del software antivirus e delle patch di sicurezza del sistema operativo e di tutti i prodotti software installati.

5.2 Dispositivi smartphone e tablet forniti dall'Università

1) I dispositivi mobili, in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni dell'Università in quanto soggetti a rischi specifici quali perdita di informazioni, accesso non autorizzato a dati personali o riservati, facilità di furto, accesso a reti wireless non sicure, possibilità di download di app con contenuto malevolo.
   La gestione dei dispositivi mobili assegnati dall'Università a collaboratori e amministratori avviene attraverso una procedura che ha lo scopo di monitorare la sicurezza di tali dispositivi e di determinare centralmente il rispetto di parte delle policy qui descritte.
2) Per ridurre il livello di esposizione alle minacce viene stabilito che:

a) ogni utente che riceve in dotazione un dispositivo mobile è responsabile del suo corretto utilizzo;
b) ogni utente, oppure il personale tecnico addetto alla gestione dei dispositivi mobili dell'Università, attiva l'impostazione del blocco dello schermo dopo pochi minuti di inattività (interazione utente-device) con sblocco attraverso password, pin o riconoscimento biometrico;
c) è fatto divieto all'utente di effettuare la disinstallazione, la disattivazione o qualsiasi manipolazione di eventuale software anti-malware installato; l'utente inoltre è tenuto a consentire l'aggiornamento dell'eventuale software anti malware attraverso la connessione dati;
d) è fatto divieto all'utente di installare software che comporti rischi per la sicurezza o di modificare funzionalità del sistema operativo del dispositivo mobile attraverso operazioni di "rooting" o "jailbreaking";
e) ogni utente e tenuto a mantenere aggiornato il sistema operativo del dispositivo assegnato;
f) al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile, sia all'interno che all'esterno delle strutture dell'Università, riponendolo in cassetti o armadi chiusi a chiave in caso di non utilizzo;
g) in caso di furto o smarrimento del dispositivo, l'utente è tenuto a segnalarlo tempestivamente al referente del Servizio IT di Ateneo che gestisce il dispositivo, in modo che gli incaricati della gestione dei dispositivi mobili dell'Università provvedano, qualora possibile, alla cancellazione remota dei dati contenuti all'interno ("remote wiping"); l'utente deve inoltre effettuare la denuncia presso le autorità competenti e farne pervenire copia al referente del Servizio IT competente;
h) poiché i dispositivi mobili sono utilizzati su reti su cui l'Università non ha nessun controllo, con conseguente rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi, l'utente è tenuto, ovunque possibile, ad utilizzare reti Wi-Fi con accesso tramite autenticazione;

i) il personale tecnico addetto alla gestione dei dispositivi mobili dell'Università, qualora lo ritenga necessario, può utilizzare uno strumento MDM (Mobile Device Management) per agevolare la gestione remota e l'aggiornamento dei dispositivi;

j) salvo specifica richiesta dell'Autorità giudiziaria la funzione degli strumenti di MDM che consente il tracciamento della posizione fisica in cui si trova il dispositivo (geo localizzazione), è disattivata.

5.3 Lavoro da remoto

1) Per l'assegnazione e l'uso degli strumenti informatici da parte degli utenti il cui rapporto di lavoro preveda la possibilità di fornire la prestazione lavorativa a distanza si rimanda al "Regolamento sullo svolgimento del lavoro a distanza".

5.4 Divieti relativi all'utilizzo di risorse informatiche assegnate

1) Le risorse informatiche assegnate possono essere esclusivamente utilizzate per le attività istituzionali e non è assolutamente consentito l'uso per fini personali.
2) In particolare, sono vietate le seguenti attività:
   a) accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
   b) diffondere prodotti informativi lesivi dell'onorabilità, individuali e collettivi;
   c) diffondere prodotti informativi di natura politica al di fuori di quelli consentiti dalla legge e dai regolamenti;
   d) diffondere, in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
   e) distribuire software che possano danneggiare le risorse informatiche, anche via e-mail;
   f) compiere attività che compromettano in qualsiasi modo la sicurezza delle risorse informatiche e della rete dell'Università;
   g) compiere attività che possano rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, CD audio e video, clonazione o programmazione di smart card;

h) utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse informatiche (ad es. cracker, programmi di condivisione), se non per scopi di didattica o di ricerca, previa autorizzazione dei referenti dei Servizi IT dell'Ateneo;
i) intraprendere azioni allo scopo di:
    i) degradare le risorse del sistema;
    ii) ottenere risorse informatiche superiori a quelle già allocate ed autorizzate;
    iii) accedere a risorse informatiche, sia dell'Università che di terze parti, violandone le misure di sicurezza;
    iv) svelare le password altrui, nonché trasmettere in chiaro, pubblicare o mandare in stampa liste di account utenti o nomi host e corrispondenti indirizzi IP delle macchine;
j) impedire ad utenti autorizzati l'accesso alle risorse informatiche assegnate;
k) utilizzare software di monitoraggio della rete in genere o intercettare pacchetti sulla rete, utilizzare sniffer o software di analisi del traffico (spyware), se non per scopi di didattica o di ricerca, previa autorizzazione dei referenti dei servizi IT dell'Ateneo;
l) accedere ai file di configurazione del sistema, farne delle copie e trasmetterle ad altri.

3) Per quanto non specificato è richiesto comunque di svolgere le prestazioni richieste in base ai principi di correttezza e buona fede.

5.5 Utilizzo dei dispositivi non forniti dall'Università

1) Gli utenti dell'Università hanno accesso ai servizi universitari esposti sulla rete esterna o resi disponibili in modalità cloud, pertanto fruibili attraverso una pluralità di dispositivi.
2) Al fine di mantenere la sicurezza dei dati di proprietà dell'Università, trattati attraverso tali dispositivi, è necessario che l'utente adotti gli accorgimenti e gli strumenti necessari per garantire la riservatezza, l'integrità e la disponibilità dei dati memorizzati sull'infrastruttura informatica dell'Università, prevenendone la memorizzazione insicura o la loro trasmissione attraverso una rete insicura, dove possono essere facilmente compromessi. Obiettivo di queste disposizioni è anche la tutela dell'utente stesso che, adottando i comportamenti indicati, non incorre in violazioni delle normative vigenti e in attribuzioni di responsabilità.
3) L'utente che accede ai suddetti servizi fuori dalla rete dell'Università è tenuto a:
    a) non memorizzare dati dell'Università su dispositivi personali, soprattutto nel caso di

documenti contenenti informazioni di natura riservata o confidenziale o nel caso di presenza di dati personali (in particolare dati di particolari categorie, così come definiti dall'art. 9 del regolamento UE 679/2016, e/o relativi a condanne penali e reati) e a non scaricare in locale gli allegati di posta elettronica. Nel caso in cui i dati dell'Università venissero inavvertitamente salvati sul dispositivo personale, l'utente è tenuto a cancellarli immediatamente dal dispositivo e da ogni possibile copia di backup;

b) impostare il blocco automatico dello schermo del dispositivo dopo pochi minuti di inattività (interazione utente-device) con sblocco attraverso password, pin o riconoscimento biometrico;
c) installare sul dispositivo un software anti malware con aggiornamento costante del database di definizione dei malware;
d) utilizzare un'utenza dedicata per l'accesso a dati dell'Università il cui uso non sia condiviso con altri soggetti, compresi i propri familiari;
e) mantenere aggiornato il dispositivo, applicando tutte le patch di sicurezza, upgrade del sistema operativo e aggiornamenti delle applicazioni installate;
f) non installare sul dispositivo applicazioni provenienti da fonti non ufficiali e/o potenzialmente pericolose per l'integrità e la sicurezza dei dati dell'Università.

5.6 Utilizzo di smartphone e tablet personali per l'accesso a dati e servizi dell'Università

1) È possibile accedere ad alcune delle risorse dell'Università a mezzo di smartphone e tablet anche di proprietà personale, sia nel caso in cui la SIM card sia di proprietà personale, sia nel caso in cui la SIM card sia fornita dall'Università.
2) Per questi casi, oltre a quanto già prescritto nel paragrafo precedente, si stabilisce che:
   a) l'utente è tenuto ad impostare il blocco automatico dello schermo dopo pochi minuti di inattività con sblocco attraverso password, pin o riconoscimento biometrico;
   b) l'utente è tenuto a non installare app al di fuori dei canali di distribuzione ufficiali e a non installare app non compatibili con la sicurezza dei dati;
   c) al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile;
   d) in caso di furto o smarrimento l'utente deve inoltre effettuare la denuncia presso le autorità

competenti e far pervenire una copia della denuncia ai referenti dei servizi IT dell'Ateneo;

e) nel caso in cui l'utente sospetti una violazione dei dati dell'Università, la presenza di un malware, oppure la compromissione del proprio dispositivo mobile personale utilizzato per accedere ai dati dell'Università, è tenuto a segnalarlo tempestivamente ai referenti dei Servizi IT dell'Ateneo, in modo che, se fosse confermata una compromissione di dati dell'Università, possano essere attivate opportune contromisure al fine di limitare i danni;
f) poiché i dispositivi mobili sono utilizzati su reti di cui l'Università non ha nessun controllo, esiste un rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi. Per tali motivi l'utente è invitato ad utilizzare preferibilmente reti Wi-Fi con accesso tramite autenticazione.

Articolo 6 - Credenziali di identificazione informatica e attivazione dei servizi

1) L'accesso alle risorse informatiche e ai dati trattati con strumentazione informatiche avviene esclusivamente previa autenticazione attraverso apposite credenziali di identificazione e limitatamente ai servizi previsti per il proprio inquadramento giuridico.

6.1 Assegnazione delle credenziali agli utenti strutturati

1) Il rilascio delle credenziali di identificazione informatica agli utenti strutturati dell'Università è conseguente alla procedura di inquadramento giuridico da parte dell'ufficio competente per la categoria di utenti considerata.
2) Il processo di rilascio delle credenziali informatiche è di competenza dei Servizi IT di Ateneo e può avvenire:
   a) a seguito di formale richiesta da parte dell'ufficio competente per l'utente in oggetto secondo le modalità individuate e pubblicate sul portale di Ateneo;
   b) in maniera automatizzata a seguito dell'inserimento dell'utente nelle anagrafiche di Ateneo, direttamente da parte dell'Ufficio competente o a seguito dell'espletamento di procedure di concorso.
3) In entrambi i casi il processo di creazione delle credenziali deve garantire la verifica, anche indiretta (ad esempio tramite SPID), dell'identità dell'utente in oggetto e la corrispondenza dei dati anagrafici inseriti, poiché le credenziali di identificazione informatica sono associate ai dati

con cui il personale è registrato nell'anagrafica dell'Università e costituiscono condizione necessaria per l'abilitazione all'utilizzo dei servizi informatici.

6.2 Assegnazione delle credenziali agli studenti

1) Il rilascio delle credenziali di identificazione agli studenti è contestuale all'immatricolazione degli stessi e avviene a seguito della loro identificazione, anche indiretta (ad esempio tramite SPID).
2) Gli studenti devono effettuare una procedura di cambio password prima di poterle utilizzare fermo restando la possibilità per l'Ateneo di fornire l'accesso ai servizi informatici di Ateneo con sistemi di autenticazione alternativi che garantiscano almeno lo stesso livello di sicurezza (ad es. SPID).

6.3 Assegnazione delle credenziali a soggetti esterni

1) Qualsiasi soggetto esterno che debba accedere ai servizi di rete e di dominio direttamente presso le sedi dell'Università o accedere tramite VPN da remoto a sistemi della rete interna, indipendentemente dall'inquadramento giuridico e/o dalla forma diretta o indiretta del proprio rapporto di collaborazione, deve essere accreditato tramite il rilascio di una credenziale informatica.
2) L'accreditamento di un soggetto esterno avviene su istanza scritta di un utente strutturato che si assume l'onere dell'identificazione del soggetto per cui richiede le credenziali.
3) L'istanza di accreditamento dovrà essere inviata ai referenti dei servizi IT dell'Ateneo, secondo le modalità indicate nel portale istituzionale e riportare, per ogni soggetto da accreditare, i minimi dati necessari per il rilascio delle credenziali incluso il termine di accreditamento.

6.4 Gestione delle credenziali

1) Ogni credenziale di identificazione informatica si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti, fatti salvi i casi di utenze amministrative utilizzate da Amministratori di Sistema e di servizi di emergenza o similari in cui vi sia la necessità di consentire l'accesso ai servizi stessi senza conoscere a priori i soggetti che vi devono accedere (es. personale addetto alla gestione emergenze, ecc.); in quest'ultimo caso la struttura di appartenenza provvede a tenere aggiornato un apposito registro con l'indicazione dei nominativi, degli orari e della postazione da cui il soggetto accede.

2) Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.
3) Ciascun utente è responsabile della sicurezza delle proprie password e deve adottare le necessarie cautele per mantenerle segrete. Le password sono strettamente personali e non devono in nessun caso essere comunicate ad altri.
4) In caso di furto delle credenziali l'utente è tenuto a seguire le procedure di seguito specificate:
   a) in caso di furto della componente riservata (password o PIN) è necessario, al primo accesso seguente al furto, cambiare la propria password o PIN e contattare il personale dei servizi IT di Ateneo per darne immediatamente comunicazione;
   b) in caso di furto o smarrimento di un dispositivo di autenticazione o di un dispositivo di firma digitale è necessario darne immediata comunicazione ai servizi IT di Ateneo e seguire le istruzioni ricevute; è inoltre necessario sporgere denuncia alle autorità competenti e trasmettere tale denuncia al certificatore.
5) Ciascun utente, quando effettua l'accesso ad un sistema per la prima volta, è tenuto a modificare e personalizzare la password di accesso composta secondo le indicazioni dei servizi ICT basate sulle più recenti policy di robustezza, tra le quali si ricorda:
   a) non impostare la password in modo che sia facilmente collegabile alla propria vita privata (per es. il nome o il cognome di familiari, la targa dell'auto, la data di nascita, la città di residenza, ecc.);
   b) non impostare come password parole comuni riportate in un vocabolario (esistono infatti programmi fraudolenti, utilizzati per la forzatura di password che si basano su ricerche sistematiche effettuate sulle parole comuni);
   c) modulare il grado di complessità della password in funzione del valore dei dati e delle risorse da proteggere; password di account con privilegi amministrativi, per esempio, richiedono complessità superiori rispetto a quelle di account non privilegiati;
   d) scegliere password che contengono combinazioni di lettere maiuscole e minuscole, numeri, caratteri speciali (per esempio: !, *, /, ?, #);
   e) non utilizzare la medesima password su sistemi differenti (per es. scegliere una password di dominio differente da quella impiegata per l'accesso a siti web esterni all'Università).

6.5 Disattivazione delle credenziali

1) Per “disattivazione delle credenziali” si intende il processo di inibizione dell’utilizzo delle credenziali e, conseguentemente, dell’accesso ai sistemi informatici e telematici dell’Università.
2) Le credenziali di autenticazione assegnate agli utenti devono essere disattivate:
   a) immediatamente alla eventuale segnalazione di morte o dalla dichiarazione di morte presunta procedendo all’eventuale recupero di dati e informazioni necessarie a consentire la continuità dell’attività dell’Ente a mezzo degli amministratori di sistema;
   b) temporaneamente, in caso di necessità e di urgenza e al fine di evitare compromissioni al normale funzionamento dei sistemi o porre termine ad attività contrarie alla normativa vigente in materia di privacy, fino alla rimozione delle cause che hanno originato il problema;
   c) a seguito di adozione di apposito atto da parte del dirigente gerarchicamente sovraordinato all’utente o del Direttore Generale nel caso di utilizzo delle credenziali assegnate in contrasto con il presente regolamento.
3) La riattivazione delle credenziali può essere eseguita:
   a) su richiesta dell’interessato, nei casi in cui esse siano associate a un dipendente in servizio;
   b) al venir meno delle cause che ne avevano resa necessaria la temporanea disattivazione;
   c) su richiesta del dirigente gerarchicamente sovraordinato nel caso di disattivazione disposta con atto del dirigente medesimo.

6.6 Autorizzazione all’uso di servizi e risorse informatiche

1) L’abilitazione di un utente all’utilizzo di applicativi, servizi e altre risorse informatiche da parte dell’Università può avvenire, salvo diversa indicazione da parte del responsabile gerarchico, anche in maniera automatizzata, sulla base dell’afferenza organizzativa, e di conseguenza può essere modificata, anche in maniera automatizzata, al variare della stessa.
2) Nel caso l’abilitazione comporti il trattamento di dati personali, resta in capo al Responsabile interno per il trattamento dei dati personali competente la designazione dell’utente incaricato del trattamento dei dati personali e ogni altro adempimento previsto dalla “Policy organizzativa dell’Università di Ferrara in materia di protezione dei dati personali”.
3) La concessione dell'abilitazione a un utente ad accedere ad ulteriori risorse informatiche dell’Università deve essere richiesta secondo le modalità indicate nel portale di Ateneo, dal

responsabile della struttura di afferenza dell'utente (o suo delegato) agli Amministratori dei Servizi Informatici corrispondenti, indicando sempre anche una data di disattivazione delle suddette abilitazioni; alla scadenza la richiesta è prorogabile con analoga modalità.

In assenza di proroga l'accesso alle risorse sarà disattivato dall'Amministratore di sistema competente, anche utilizzando modalità automatizzate dove disponibili.

4) Sono ammissibili eccezioni alle norme sopra indicate a seguito di istanze motivate e approvate dal Rettore, dal Direttore Generale, da un Direttore di Dipartimento o da un dirigente.

6.7 Rimozione autorizzazione all'uso di servizi e risorse informatiche

1) L'accesso agli applicativi, ai servizi ed alle risorse informatiche dell'Università può essere disabilitato, anche in maniera selettiva e automatizzata, in considerazione di particolari condizioni, quali la variazione dello stato giuridico dell'utente o la modifica dello stato di carriera degli studenti.
2) Nel caso di cessazione del diritto di un incaricato ad accedere a una o a più risorse informatiche dell'Università, è onere del responsabile della struttura di afferenza dell'utente (o suo delegato), assicurarsi, presso gli Amministratori dei Servizi Informatici corrispondenti, dell'avvenuta disattivazione delle autorizzazioni associate a tale incaricato.
3) In caso di sostituzione del responsabile di una struttura, il responsabile entrante è tenuto a rivedere le assegnazioni di servizi a tutti i collaboratori interni ed esterni della struttura.
4) L'accesso alle risorse informatiche dell'Università è comunque consentito agli utenti abilitati, in relazione al ruolo ricoperto, per il solo periodo di durata del rapporto con l'Università; in particolare deve essere inibito l'accesso ai principali applicativi e risorse informatiche necessari per lo svolgimento della prestazione lavorativa entro 30 giorni dall'eventuale data di interruzione del rapporto di collaborazione con l'Università.
5) Fanno eccezione i servizi che devono obbligatoriamente rimanere attivi per periodi più lunghi (es: consultazione cedolini e carriera universitaria etc.) e dei servizi di posta elettronica, relativi allo spazio personale di archiviazione di file ed eventuali altri servizi per i quali, in considerazione della particolarità del servizio, può essere previsto un periodo superiore prima della disattivazione, anche con fruizione in modalità ridotta, purché questo non comporti costi aggiuntivi per l'Ateneo.

Resta garantita la possibilità per l'utente di richiedere in qualsiasi momento la disattivazione di detti servizi e la cancellazione dei relativi dati purché la conservazione degli stessi non sia richiesta da altra norma.

6) Le modalità e le tempistiche di disattivazione dell'accesso ai servizi e alle risorse informatiche e di eventuale cancellazione dei dati sono decise dall' RTD o suo delegato in funzione del ruolo ricoperto dall'utente, dalle tecnologie utilizzate, degli accordi con eventuali fornitori e dei relativi costi per l'Università e sono pubblicate nella sezione Servizi Online del portale Web di Ateneo.
7) Sono possibili deroghe in caso di particolari necessità, che devono essere approvate dal Direttore Generale per quello che riguarda il PTA e dal Rettore o suo delegato per quanto riguarda tutte le altre tipologie di utenti.

Articolo 7 - Utilizzi della rete dell'Università

1) Al fine di prevenire l'accesso ai sistemi informatici da parte di soggetti non autorizzati è fatto divieto di:
   a) modificare la configurazione di rete sulla propria postazione di lavoro o su apparati di cui si è responsabili. Questa può essere modificata od autorizzata solo dall'Amministratore di sistema;
   b) utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente;
   c) connettere ad Internet, tramite reti wi-fi, modem o altri apparati di accesso remoto non espressamente autorizzati, strumentazioni informatiche collegate alla rete interna dell'Università;
   d) connettere alla rete cablata interna dell'Università strumenti elettronici personali o comunque non espressamente autorizzati;
   e) connettere alla rete interna dell'Università access point o altri apparati di rete non espressamente autorizzati come ad esempio hub o miniswitch per sottoreti PC e stampanti;
   f) accedere ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi;
   g) utilizzare strumenti di sniffing, cracking o scanning e introdurre o diffondere volontariamente programmi nocivi (per es. virus, worm, spyware, ecc.) nella rete o nei

sistemi, ove non sia assolutamente necessario per scopi di didattica o di ricerca e dopo aver ricevuto espressa autorizzazione in merito da parte dei referenti dei Servizi IT dell'Ateneo.

7.1 Modalità di accesso alla rete

1) Si definiscono, per gli scopi del presente regolamento, i seguenti luoghi di accesso alla rete:
   a) uffici e studi: luoghi riservati al personale strutturato dell'Università ed eventualmente a collaboratori temporanei;
   b) laboratori didattici: luoghi dedicati alle esercitazioni didattiche;
   c) laboratori di ricerca: luoghi dedicati all'attività di ricerca;
   d) biblioteche: luoghi di consultazione di materiale librario, cartaceo o digitale;
   e) spazi comuni: luoghi di passaggio o di incontro dove siano installati terminali di accesso ai servizi di rete;
   f) VPN (Virtual Private Network).

7.1.1 Accesso senza login

1) L'accesso senza login alla rete Universitaria è permesso solo all'interno di locali ad accesso non libero, in particolare: Uffici, Studi, Laboratori di ricerca, Biblioteche. Possono accedere senza login: il personale docente e tecnico-amministrativo, dottorandi, specializzandi, assegnisti, i soggetti esterni con rapporti di collaborazione, di docenza e di ricerca con l'Ateneo comunque preventivamente identificati e autorizzati.

7.1.2 Accesso con login

1) L'accesso con login alla rete Universitaria è permesso all'interno di tutte le strutture dell'Università.
2) Possono accedere mediante login tutti gli utenti, compresi gli studenti, in possesso di credenziali di identificazione, fornite secondo le modalità descritte nell'articolo 6.
3) Il sistema di accesso con login è attivo anche per utenti connessi a risorse esterne alla rete Universitaria che necessitano di un indirizzo privato per poter accedere alle varie risorse dell'Università; a tale fine è possibile utilizzare un servizio di VPN.
4) L'autenticazione viene eseguita mediante la redirezione verso un'apposita pagina Web di autenticazione indipendentemente dalla richiesta Web effettuata. L'autenticazione avviene

tramite lo username e la password utilizzate per accedere ai servizi dell'Università. All'atto dell'autenticazione vengono messi a disposizione solo un ristretto numero di servizi.

5) I Servizi IT di Ateneo mantengono traccia di tutte le attività verso Internet riconducibili al dispositivo a cui l'utente è associato. Tali dati vengono conservati secondo la normativa vigente e possono essere forniti su richiesta all'autorità giudiziaria ma ne è vietato qualsiasi utilizzo al di fuori della verifica della sicurezza e della funzionalità dei servizi di rete, effettuata da personale espressamente formato e autorizzato. In particolare, è vietato qualsiasi possibile utilizzo ai fini del monitoraggio dell'attività lavorativa.

Articolo 8 - Servizi Cloud di produttività

1) I servizi cloud devono essere utilizzati esclusivamente per finalità lavorative, di ricerca o di studio.
2) È vietato utilizzare i servizi cloud per attività illecite, diffamatorie, offensive o dannose per l'ateneo o per terzi.
3) È vietato condividere dati sensibili o riservati con soggetti esterni all'ateneo senza le opportune autorizzazioni; i dati personali devono essere trattati nel rispetto della normativa sulla protezione dei dati personali.
4) I servizi disponibili e le quote di spazio disponibile agli utenti sono definiti dall'Ateneo e pubblicate nella sezione "Servizi Online" del portale.

   L'Ateneo si riserva di modificare i servizi e le risorse assegnate alle categorie di utenti in base alle disponibilità, previa comunicazione via e-mail e/o pubblicazione delle nuove quote nell'apposita pagina sul portale di Ateneo.
5) In caso di superamento della quota concessa da parte degli utenti, i servizi Cloud verranno bloccati in sola lettura fino al rientro nei limiti stabiliti e ne verrà data comunicazione all'utente all'indirizzo mail istituzionale.

   Trascorsi 10 giorni senza risposta l'Ateneo si riserva il diritto di cancellare i dati degli account che non rientrano nelle quote stabilite.
6) Trascorso un periodo di un anno senza che l'utente abbia fatto accesso ai propri dati l'Ateneo si riserva il diritto di disattivare l'accesso ai predetti servizi e di cancellare i dati stessi liberando lo spazio concesso.

7) Per una maggiore sicurezza contro la perdita di dati l'Ateneo attiva, dove possibile, un servizio di conservazione ed eDiscovery dei dati in cloud.

8.1 Posta elettronica

1) La casella di posta elettronica viene fornita dall'Università quale strumento di supporto per lo svolgimento dell'attività lavorativa, di studio e di ricerca e delle attività che siano strumentali e connesse alla stessa.
2) Le caselle di posta elettronica sono assegnate come servizio di base a ciascun utente al momento del rilascio delle credenziali di identificazione informatica e rientrano tra gli strumenti assegnati dal sistema informativo dell'Università.
3) Ai collaboratori esterni la casella di posta è assegnata su richiesta motivata del Responsabile della struttura a cui il collaboratore afferisce qualora risulti indispensabile per svolgere attività che non sia possibile svolgere con e-mail personali e/o aziendali. La richiesta di attivazione dei servizi di posta personale dell'Università ai collaboratori esterni accreditati deve essere richiesta ai Servizi IT di Ateneo e segue le procedure di attivazione precedentemente descritte nell'articolo 6.3 per l'assegnazione delle credenziali a soggetti esterni.
4) Per attivare ulteriori indirizzi di posta elettronica, per attività di gruppo o di progetto, gli utenti strutturati possono inoltrare richiesta motivata ai Servizi IT di Ateneo.
5) Le caselle di posta elettronica certificata (PEC) sono assegnate alle strutture dell'Università per le quali sono previsti processi di comunicazione istituzionale con soggetti terzi. La richiesta di attivazione di caselle PEC segue le procedure di attivazione precedentemente descritte.
6) L'amministrazione degli utenti che accedono a caselle di struttura, di gruppo o di progetto è assegnata ai responsabili delle strutture competenti o a loro delegati.
7) L'accesso al contenuto della casella di posta elettronica personale è consentito solo all'utente assegnatario. L'accesso da parte di terzi alla casella personale di un utente è vietato, salvo quanto indicato nell'articolo 17. È inoltre fatto salvo l'eventuale adempimento a richieste dell'Autorità giudiziaria.
8) Nel caso di specifica e circostanziata segnalazione relativa a un utilizzo improprio di una casella di posta istituzionale l'accesso può essere effettuato allo scopo di evitare la distruzione di informazioni necessarie per lo svolgimento di un procedimento disciplinare, su richiesta del

soggetto titolare del procedimento stesso.

8.1.1 Utilizzo della posta elettronica

1. La posta elettronica deve essere utilizzata esclusivamente per le specifiche finalità della propria attività lavorativa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi e degli altri utenti dell'ente e dei processi lavorativi, adottando comportamenti idonei a prevenire la perdita di confidenzialità di dati riservati e l'utilizzo non appropriato di beni dell'Università.
2. La casella di posta elettronica certificata (PEC) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali. Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione costituisce comunicazione di dati personali e, come tale, deve essere effettuata ai sensi della normativa vigente oppure a riscontro di una istanza dell'interessato ai propri dati personali.
3. Nel caso di utilizzo della posta elettronica certificata (PEC) per la trasmissione di dati personali comuni (vale a dire non particolari, ovvero non dati di particolari categorie e/o relativi a condanne penali e reati) il cui trattamento sia di titolarità dell'Università, l'utente dovrà solo accertarsi della legittimità del destinatario a ricevere i dati personali che intende inviare; qualora venisse utilizzata, invece, la casella di posta elettronica "ordinaria" l'utente dovrà accertarsi, oltre che della legittimità del destinatario alla ricezione dei dati personali, anche dell'identità dello stesso, che si intende certa se:
   a) ha presentato via e-mail una richiesta per l'invio dei dati firmata digitalmente;
   b) oltre alla richiesta di dati presentata via e-mail o telefonicamente, ha trasmesso, anche via mail, una copia semplice di un documento di identità in corso di validità.
4. Nel caso di ragionevole certezza sull'identità del richiedente (ad esempio perché il richiedente è conosciuto personalmente) oppure in casi di improrogabile urgenza, l'accertamento dell'identità del ricevente può essere effettuata per via telefonica.
5. Le modalità tecniche cambiano in relazione alla tipologia dei dati personali che si intende inviare. Nei casi in cui sia necessario inviare dati di particolari categorie e/o relativi a condanne penali e reati, verificata da parte dell'utente la liceità del trattamento ai sensi della normativa vigente, la comunicazione deve essere effettuata secondo una delle seguenti modalità:
   a) utilizzando opportune tecniche di cifratura avvalendosi di strumenti preventivamente

concordati con i Servizi IT di Ateneo;

b) impiegando soluzioni alternative che rendano i dati temporaneamente inintelligibili e permettano di identificare gli interessati solo in caso di necessità (per es. mandare in e-mail separate i dati di particolari categorie e/o relativi a condanne penali e reati dagli altri dati personali, utilizzare codici identificativi al posto di nome e cognome, ecc.).

8.2 Prevenzione da malware

1) Al fine di prevenire le minacce rappresentate da software malevoli (per es. virus, worm, spyware, ransomware ecc.) che potrebbero essere contenuti in email o negli allegati delle email stesse, si forniscono le seguenti indicazioni:
   a) "Spam" è il termine con cui si indica l'invio incessante, ma soprattutto indesiderato, di messaggi pubblicitari o parti delle cosiddette catene di S. Antonio ad un gran numero di utenti contemporaneamente. Le operazioni di invio possono realizzarsi via e-mail o tramite i gruppi di discussione. A titolo preventivo si raccomanda di:
      i) non rispondere mai a messaggi di presunto spamming, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
      ii) limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail su siti web pubblici (per es. forum, mailing list, ecc.);
      iii) non rispondere o inoltrare e-mail di c.d. "Catene di S. Antonio", ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
      iv) non configurare la conferma di lettura in modalità automatica.
   b) Il phishing è una tecnica di attacco che sfrutta e-mail e siti web "fantasma", del tutto simili nell'aspetto agli originali, per ingannare l'utente e carpire informazioni confidenziali o personali. È necessario, quindi, prestare massima attenzione alle e-mail che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi, ecc.).
   c) In caso di dubbi sulla qualità di messaggi e-mail, si raccomanda di contattare l'indirizzo di

posta dedicato alle problematiche di sicurezza informatica dell'Università helpdesk@unife.it.

Articolo 9 - Navigazione in internet

1) L'Università fornisce l'accesso a Internet a supporto dello svolgimento dell'attività lavorativa, di ricerca, di didattica e delle attività che siano strumentali e connesse alle stesse e per questo se ne prescrive un utilizzo pertinente alle specifiche finalità, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.
2) È fatto divieto di:
   a) scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, verificare la provenienza e l'autenticità del software (per es. tramite meccanismi di firma digitale);
   b) utilizzare siti pubblici di condivisione dei file e di archiviazione online forniti da provider che non assicurano strumenti di protezione adeguati;
   c) caricare su servizi o siti web terzi di condivisione, archiviazione o backup online non espressamente autorizzati dall'Università documenti inerenti all'attività lavorativa o istituzionale, soprattutto se contenenti dati personali, di particolari categorie e/o relativi a condanne penali e reati.

Articolo 10 - Protezione antivirus

1) L'utente utilizzatore delle risorse informatiche dell'Università è tenuto ad adottare le necessarie cautele al fine di ridurre il rischio di infezione virale della propria o altrui postazione di lavoro. È fatto divieto, ai soggetti che sono amministratori di postazione di lavoro, di rimuovere il programma antivirus installato su di essa o di alterarne la configurazione. Gli utenti sono tenuti a segnalare problemi eventualmente riscontrati sulla corretta installazione e funzionamento del programma antivirus presente sulla propria postazione di lavoro.
2) Prima di utilizzare supporti rimovibili, gli utenti sono tenuti a verificare la presenza di eventuali virus in esso contenuti.
3) A seguito di segnalazione della presenza di un virus da parte del software antivirus si prescrive di:

a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) segnalare tramite helpdesk@unife.it l'evento ai Servizi IT di Ateneo;
c) non inviare ad altri utenti i messaggi di posta elettronica contenenti segnalazioni del virus;
d) scollegare il dispositivo dalla rete di Ateneo (es: rimuovendo fisicamente il cavo di rete, o mettendo in "modalità aereo" i dispositivi mobili) fino a successiva comunicazione del personale deputato a gestire l'incidente.

Articolo 11 - Gestione dei log

1) I sistemi informativi dell'Università sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti, ed in particolare dei requisiti di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.
2) Alcune attività dell'utenza sono soggette a logging: ciò significa che alcune operazioni eseguite dagli utenti dei sistemi informativi vengono memorizzate in formato elettronico e conservate per un certo periodo di tempo. Il logging è necessario per ragioni di sicurezza: il livello del logging dei diversi servizi, ossia il livello di dettaglio dei dati memorizzati, è funzionale unicamente alla verifica della sicurezza con la quale i servizi sono erogati e per nessun motivo viene utilizzato per il controllo dell'attività lavorativa.
3) Di seguito vengono dettagliate le tipologie di log raccolti e conservati:
   a) log della navigazione web, del firewall e del server di posta: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze; scopo ulteriore della raccolta, per quel che riguarda la navigazione web, è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Università al fine di svolgere la propria attività lavorativa;
   b) log delle segnalazioni ed alert di tutte le tipologie di sistema antimalware: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
   c) log degli accessi degli Amministratori di Sistema ai sistemi amministrati: tale raccolta è

motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli Amministratori di Sistema;

d) log degli accessi degli utenti ai servizi di rete: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
e) log degli accessi degli utenti al sistema di stampa e delle operazioni effettuate: tale raccolta deriva dalla necessità di poter identificare, anche a posteriori, incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze; scopo ulteriore della raccolta è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Università al fine di svolgere la propria attività lavorativa;
f) log delle attività svolte da utenti e amministratori di sistema nell'ambito di alcuni software complessi: tale raccolta è motivata dalla necessità di poter individuare anche a posteriori eventuali violazione delle policy e audit sulla correttezza dei dati gestiti dal software stesso;
g) log delle chiamate telefoniche su terminali VoIP, finalizzato al monitoraggio dei costi, alla verifica della funzionalità del sistema e alla verifica di eventuali accessi abusivi o usi non consentiti.

4) Il tempo di conservazione di tutte le tipologie di log sopra elencate è fissato, salvo i casi in cui la normativa preveda un tempo superiore, ad un periodo di un anno, previo accordo con le rappresentanze sindacali di Ateneo.
5) Fanno eccezione i log di funzionamento del sistema di posta elettronica, il cui tempo di ritenzione, in funzione della particolarità dei dati trattati, è di 90 giorni, previo accordo con le rappresentanze sindacali di Ateneo.
6) Per tutte le tipologie di log per cui non sia possibile raggiungere un accordo con le rappresentanze sindacali di Ateneo, il tempo di ritenzione degli stessi è fissato a 21 giorni, sempre con l'eccezione dei casi in cui specifiche normative prevedano un tempo superiore.
7) La conservazione dei log è motivata dalla necessità del loro utilizzo per la verifica annuale delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali e di avere una policy di retention dei log uniforme per tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.

Articolo 12 - Prevenzione e gestione degli incidenti di sicurezza informatica

1) Al fine di prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile è necessario operare tempestivamente e in uno spirito di collaborazione. Qualora si ravvisassero violazioni di sicurezza interna o eventi che possano portare a credere che vi sia stata una elusione delle misure di sicurezza previste, è necessario segnalare tempestivamente l'accaduto al Gruppo per la gestione della sicurezza ICT e dei data breach (G-ICT), attraverso una mail all'indirizzo g-ict@unife.it e comunicare l'incidente ai servizi IT di Ateneo o ad un tecnico informatico in servizio nell'Ateneo.
2) In un'ottica di prevenzione degli incidenti di sicurezza, è necessario attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna dell'Università.

Articolo 13 - Protezione dei dati trattati senza l'utilizzo di strumenti elettronici

1) L'accesso ai dati trattati senza l'utilizzo di strumenti elettronici è consentito, come per i trattamenti di dati personali effettuati con mezzi elettronici, esclusivamente al personale espressamente incaricato.
2) È assolutamente necessario raccogliere prontamente, nel caso si utilizzino stampanti di rete o fax ubicati in locali comuni (per es. corridoi), i documenti stampati o ricevuti via fax, soprattutto se contenenti dati personali, in modo da preservare la riservatezza del contenuto.
3) È ugualmente necessario, ai fini della tutela dei dati personali trattati nell'espletamento delle proprie mansioni, assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo dell'Università, non siano lasciati a vista sulla scrivania ma conservati in cassetti o armadi chiusi a chiave o in locali a cui sia possibile inibire l'accesso al personale non autorizzato.
4) È inoltre necessario prevedere la disponibilità delle stesse, durante la propria assenza dall'attività lavorativa, in modalità controllata e sicura (esempio: copia delle chiavi depositate in segreteria, registro di presa in carico e di riconsegna, etc.).
5) Nei casi in cui atti o documenti contengano dati di particolari categorie e/o relativi a condanne penali e reati, deve essere prevista apposita procedura per la conservazione in archivi ad accesso

selezionato, disciplinando modalità di ingresso tali da consentire l'identificazione degli utenti che vi accedono. È necessario custodire opportunamente i documenti prelevati per impedire l'accesso improprio da parte di persone non autorizzate. In particolare, essi non dovranno rimanere incustoditi nemmeno per brevi periodi, provvedendo eventualmente a riporli in armadi o cassetti chiusi a chiave. Al termine del trattamento, l'utilizzatore avrà cura di ricollocare i documenti nell'archivio di provenienza.

Articolo 14 - Trattamento dei dati sensibili e/o riservati nell'ambito della ricerca scientifica

1) Considerando le necessità di contemperare il diritto alla libertà di ricerca con la protezione dei dati riservati o oggetto di proprietà intellettuale e con il diritto alla protezione dei dati personali, e considerando i vincoli normativi, in particolare il D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e ss.mm.ii (che contempla allegati specifici per l'ambito della ricerca), è necessario, per ogni attività che coinvolga il trattamento di dati personali o di dati e informazioni riservate:
   a) effettuare una opportuna valutazione del rischio del trattamento dei dati e, se necessario, una valutazione di impatto sulla protezione dei dati personali (DPIA);
   b) ove previsto, tenere apposito registro dei trattamenti dei dati personali;
   c) ove necessario fornire adeguata informativa per il trattamento dei dati personali;
   d) limitare l'accesso ai suddetti dati al solo personale interessato, dopo apposita formazione in merito alle corrette modalità di trattamento e, se prevista, apposita nomina di addetto al trattamento;
   e) consentire l'accesso ai dati solo con l'utilizzo di credenziali di accesso nominali e, ove possibile, utilizzando soluzioni di autenticazione multi-fattore;
   f) prediligere, ove possibile, soluzioni di crittografia dei dati presenti su supporti informatici;
   g) proteggere adeguatamente l'accesso ad eventuale documentazione cartacea o in altra forma.
2) Qualora non si disponga di adeguate competenze tecniche, è necessario rivolgersi ai referenti per i servizi IT dell'Ateneo per avere informazioni in merito alle soluzioni tecnologiche più indicate e ai referenti per la protezione dei dati personali per avere informazioni più dettagliate in merito agli adempimenti normativi in materia.

3) Nel caso in cui, per lo svolgimento della ricerca, sia necessario l'accreditamento dell'Università di Ferrara presso un qualsiasi ente od organizzazione è necessario contattare i referenti per i servizi IT dell'Ateneo per la valutazione dei requisiti tecnici necessari.

Articolo 15 - Acquisizione di nuovi applicativi

1) Per l'acquisizione di qualsiasi tipologia di software è necessario il rispetto delle normative previste in proposito per la pubblica amministrazione.

   A tal fine, prima di effettuare qualsiasi acquisizione di un prodotto software, è necessario contattare con congruo anticipo il servizio IT competente di Ateneo che verificherà la corrispondenza dell'applicativo individuato con la normativa vigente, e la disponibilità del personale competente sia per la valutazione che per tutte le successive fasi di integrazione con gli altri applicativi in uso, configurazione, avvio e successiva assistenza.
2) In caso contrario non sarà garantita l'assistenza nelle predette attività, senza le quali potrebbe non essere possibile utilizzare il software acquisito, oltre ad esporre l'Università a possibili sanzioni da parte degli organismi competenti, per le quali l'Università si riserva il diritto di rivalsa sul soggetto che non ha rispettato quanto previsto dal presente regolamento.

Articolo 16 - Policy di gestione delle informazioni e della conoscenza

1) L'Università di Ferrara individua nella condivisione di dati e informazioni non solo uno strumento indispensabile a favorire la semplificazione e la digitalizzazione dei processi e delle attività, ma anche un presupposto all'adempimento degli obblighi di trasparenza dell'attività amministrativa e un elemento imprescindibile nell'implementare efficaci strumenti di controllo e monitoraggio delle performance, utili alla governance a poter impostare politiche di gestione più efficaci e tempestive.
2) Per questo motivo lo sviluppo, l'aggiornamento e l'acquisizione di applicativi e strumenti software deve essere conforme alle "Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni" e alle "Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici" emanate da AgID; deve inoltre espressamente tenere in considerazione come requisito essenziale la più ampia interoperabilità tra tutti gli strumenti in uso in Ateneo al fine della massima condivisione delle informazioni e della conoscenza, sempre

contemperando le esigenze di sicurezza informatica e i requisiti di riservatezza e limitazione nel trattamento dei dati personali, secondo il paradigma di privacy by design e privacy by default.

Articolo 17 - Recupero dei dati per fini istituzionali in assenza dell'utente

1) In caso di assenza programmata o improvvisa e imprevista di un dipendente, l'Università è tenuta a garantire l'operatività organizzativa e amministrativa, nel rispetto del diritto del lavoratore alla tutela della propria sfera di riservatezza anche nell'ambito della propria attività lavorativa. In linea con il Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" e degli orientamenti sia del Garante stesso sia giurisprudenziali in materia, l'Università, nell'esercizio delle proprie prerogative organizzative, accede prioritariamente con modalità e strumenti che non comportano un accesso diretto ai dati personali e alle informazioni trattate dall'utente assente e quindi a funzionalità che meno comprimono il diritto alla riservatezza.
2) La possibilità di accedere ai messaggi di posta oppure a file o cartelle presenti nello spazio personale in cloud o sulle risorse informatiche assegnate ad un utente può avvenire soltanto in casi di effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa. Soltanto in tale caso di emergenza sono previste e di seguito esplicitate le procedure che contemplano l'accesso alla casella di posta elettronica e ai dati dello spazio personale dell'utente su istanza motivata del Responsabile della Struttura, approvata dal Dirigente gerarchicamente sovraordinato all'utente e trasmessa al referente del Servizio IT competente.
3) È comunque fatto divieto di accedere ai messaggi di posta elettronica e a file o cartelle che, già dall'oggetto e/o dalla denominazione e/o dalle proprietà, possano far prefigurare un contenuto riconducibile a informazioni personali non riconducibili ad attività lavorativa che, anche in tale sede, devono ricevere la dovuta tutela.
4) È necessario evitare, ove possibile, la conservazione di cartelle e documenti di lavoro sui dischi locali dei personal computer, dei portatili e di smartphone e tablet, e qualora fosse necessario, di adottare idonee misure di sicurezza, quali la cifratura dei dati, al fine di limitare i possibili rischi in termini di confidenzialità, integrità e disponibilità dei contenuti prodotti da ciascun utente.
5) Nei casi in cui l'Università abbia necessità di accedere a contenuti indispensabili ad assicurare la continuità dell'attività lavorativa che l'utente abbia incautamente memorizzato sul disco locale

della postazione di lavoro assegnata, si applicano per analogia le regole stabilite nei paragrafi seguenti.

17.1 Recupero dati in caso di delega

1) In caso di assenze programmate (ad esempio in caso di ferie) e qualora vi siano esigenze di assicurare la continuità dell'attività lavorativa, l'utente può condividere file o cartelle a mezzo del cloud o delle risorse di rete in favore di altro utente o gruppo di utenti, che siano autorizzati a trattare i dati condivisi.
2) I soggetti delegati faranno accesso ai soli file/cartelle necessari ad assicurare la continuità dell'attività lavorativa.

17.2 Recupero dati in assenza di delega

1) Qualora l'utente assente non avesse delegato altri soggetti ad accedere ai propri contenuti, si prevede, sia nel caso in cui l'assenza sia programmata, sia nel caso in cui non lo sia, sia in caso di decesso, quanto segue:
   a) il Responsabile della Struttura di appartenenza dell'utente assente che, esclusivamente per le succitate esigenze, intenda accedere a messaggi (inclusi gli eventuali allegati) presenti nella casella di posta elettronica o a file/cartelle presenti nel cloud o sulle risorse di rete, assegnate allo stesso, deve effettuare la richiesta che viene approvata dal Dirigente gerarchicamente sovraordinato all'utente e trasmessa al referente del Servizio IT competente;
   b) l'accesso può essere autorizzato esclusivamente agli amministratori di sistema dell'Università;
   c) l'amministratore di sistema è designato quale incaricato del trattamento di dati personali che sia strettamente necessario effettuare al fine di adempiere ai compiti assegnatigli con l'istanza di cui alla lettera a);
   d) è fatto divieto all'Amministratore di sistema incaricato di accedere ai messaggi di posta elettronica o file/cartelle che, già dall'oggetto, possano far prefigurare un contenuto riconducibile a informazioni personali non relative all'attività lavorativa del soggetto assente;
   e) al termine della procedura di accesso e dopo aver trasmesso al Responsabile di Struttura

istante i contenuti richiesti, l'Amministratore di sistema incaricato redige apposito verbale delle operazioni effettuate che consegnerà agli atti della struttura;

f) salvo il caso di decesso, l'utente ha diritto di prendere visione del verbale delle operazioni effettuate.

Articolo 18 - Recupero dei dati della persona deceduta per fini non istituzionali

Non è consentito accedere ai dati della casella di posta elettronica o a file/cartelle presenti nel cloud o alle risorse di rete assegnate alla persona deceduta per fini non istituzionali, salvo il caso in cui, su richiesta degli eredi, si debba accedere a specifici documenti al fine di garantire la protezione del diritto d'autore e/o di altri diritti connessi al suo esercizio ai sensi di legge.

Articolo 19 - Controlli e sanzioni

19.1 Controlli

1) I referenti per i Servizi IT dell'Ateneo o altri soggetti delegati dal Titolare per il trattamento dei dati personali effettuano controlli, anche preventivi, sul corretto uso e funzionamento degli strumenti informatici nel rispetto dei diritti e delle libertà fondamentali degli utenti o dei soggetti esterni che utilizzano strumenti informatici dell'Università al fine di evitare usi impropri dei sistemi messi loro a disposizione.
2) Possono essere effettuati controlli automatizzati sul traffico di rete volti a inibire l'accesso a siti o categorie di siti di palese natura non istituzionale.
3) I controlli sulle attività svolte mediante utilizzo dei sistemi informatici sono ammessi nei seguenti casi:
   a) quando previsti da fonte normativa o regolamentare;
   b) nel caso in cui si verifichino eventi dannosi o situazioni di pericolo non impediti da preventivi accorgimenti tecnici;
   c) su segnalazione dell'Autorità Giudiziaria;
   d) nel caso in cui, nell'ambito delle ordinarie attività di gestione dei sistemi informativi di competenza, siano rilevati file illegali o dal contenuto palesemente non istituzionale;
   e) nell'ambito di controlli saltuari a campione per le finalità di cui al paragrafo precedente.
4) Dai suddetti controlli sono esclusi gli strumenti utilizzati direttamente dal lavoratore, quali ad

esempio possono essere: computer in dotazione, telefono, smartphone e tablet.

5) Nei casi in cui, a seguito di un controllo, si rilevino comportamenti illegali o non istituzionali, i referenti dei Servizi IT dell'Ateneo o altri soggetti delegati dal Titolare potranno intervenire valutando se:
   a) inviare avvisi collettivi o individuali in cui verranno segnalati i comportamenti non corretti;
   b) rimuovere i file, senza alcun preavviso all'utente, nei casi in cui i file possano limitare l'utilizzo di risorse o possano recar danno all'Università;
   c) inibire l'accesso a siti o categorie di siti di palese natura non istituzionale;
   d) informare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, il legale rappresentante o il dirigente del personale, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni di cui al paragrafo successivo "sanzioni".

19.2 Sanzioni

1) I comportamenti in violazione della normativa vigente e del presente regolamento che hanno una rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, saranno sanzionati secondo le forme e le modalità previste dai rispettivi ordinamenti del personale coinvolto.
2) Tali comportamenti sono segnalati al dirigente del personale per quello che riguarda il PTA e al Rettore per quanto riguarda tutte le altre tipologie di utenti, i quali valuteranno le modalità di intervento più idonee, anche a tutela di eventuali danni economici e/o di immagine subiti dall'Università.

Articolo 20 - Norme finali

Il presente Regolamento è emanato con decreto rettorale ed entra in vigore il 15° giorno successivo alla data di pubblicazione nell'Albo Online.

Glossario

Termine/Acronimo	Descrizione
Autenticazione	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente che accede ai sistemi informativi.
Cracking (strumenti di)	software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.
Dati personali	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati di particolari categorie	dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
Dispositivo mobile	sistema di elaborazione che può essere spostato e trasportato. Nel contesto del presente documento, per dispositivo mobile si intende solo “smartphone” o “tablet”, mentre negli altri casi si parla esplicitamente di “computer portatile”, o “postazione

	di lavoro portatile”
Identificazione informatica	la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.
Incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
Jailbreaking	Operazione con la quale un utente rimuove le protezioni impostate dal produttore del dispositivo, riuscendo così ad eseguire operazioni normalmente non consentite.
Password	sequenza di caratteri alfanumerici che costituisce la chiave d'accesso ad un sistema protetto. In assenza di altri dispositivi, la password costituisce il meccanismo di sicurezza base per la protezione dell’accesso a risorse informatiche.
Phishing	tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).
Postazione di lavoro	Il pc o il portatile comprensivo di tutte le periferiche di input e output (mouse, tastiera, webcam, video, stampante collegata) che costituiscono la dotazione hardware assegnata ad un utente
Ransomware	tipo di malware che limita l'accesso del dispositivo che infetta

	(per esempio cifrando i dati), richiedendo un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione
Responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Rooting	Operazione attraverso la quale un utente può ottenere i privilegi di amministratore di sistema di un dispositivo mobile, riuscendo così ad eseguire operazioni normalmente non consentite
Scanning	attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.
Sniffing (strumenti di)	software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.
Spamming	l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.
Spyware	software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.
Supporto rimovibile	dispositivo su cui è possibile registrare dati che può essere facilmente rimosso dal sistema che lo legge/scrive, trasportato in altri luoghi e collegato ad altri sistemi. Esempi di supporti rimovibili sono: chiavette USB, hard disk esterni, CD ROM.

Titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
Worm	programma in grado di autodiffondersi sulla rete e verso altri sistemi.
Virus	programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.
VPN	Una Virtual Private Network (Rete privata Virtuale) è una tecnologia che permette di stabilire una connessione sicura e cifrata con una rete privata, ad esempio la rete di Ateneo, su una rete meno sicura, tipicamente Internet