Regolamento di sicurezza delle informazioni e utilizzo delle risorse informatiche

Glossario

Incidente informatico	Per incidente informatico si intende una classe generale di imprevisti e malfunzionamenti (anche accidentali) hardware o software.
Malware	Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.
Data Breach	Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Dominio di Ateneo	nome univoco posto dopo il simbolo @ negli indirizzi email che identifica l'organizzazione che lo gestisce (es.: unipr.it).
Cloud computing	è un modello di infrastrutture informatiche che consente di disporre, tramite internet, di un insieme di risorse hardware e software (ad es. reti, server, risorse di archiviazione, applicazioni software) che possono essere rapidamente erogate come servizio, consentendo all'utente di non dover preoccuparsi, ad esempio, di come configurare e installare un software sulla propria macchina. Le classi di servizio più comuni che caratterizzano i servizi cloud sono IaaS, PaaS e SaaS. Tali servizi possono erogati agli utenti secondo diverse modalità di fruizione: public cloud, private cloud e hybrid cloud.
ICT	information and communications technology, sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese).
VPN	virtual private network, rete di telecomunicazioni privata che garantisce diversi tipi di protezione dei dati, tra cui confidenzialità, integrità, autenticazione e protezione dai replay attack (forma di attacco informatico che ha come bersaglio reti informatiche allo scopo di impossessarsi di una credenziale di autenticazione).
Connessioni HTTPS/TSL/SFTP	protocolli per la comunicazione sicura attraverso una rete di computer utilizzato su Internet.
LOG	registrazione sequenziale e cronologica delle operazioni effettuate, da un utente, un amministratore o automatizzate, man mano che vengono eseguite dal sistema o applicazione.
IDS	Intrusion Detection System è un dispositivo software e/o hardware utilizzato per identificare e/o prevenire accessi non autorizzati ai computer o alle reti locali.
Router	dispositivo di rete usato come interfacciamento tra sottoreti diverse come per esempio il collegamento alla rete internet.
Wi-Fi	è un insieme di tecnologie per reti locali senza fili (WLAN) basato sugli standard IEEE 802.11, il quale consente a più dispositivi (per esempio personal computer, smartphone, smart TV, ecc.)di essere connessi tra loro tramite onde radio e scambiare dati.
NAS	network attached storage è un dispositivo collegato alla rete la cui funzione è quella di consentire agli utenti di accedere e condividere uno spazio comune (una memoria di massa).
Indirizzo IP	Internet protocol address è un numero che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza

	l'Internet Protocol come protocollo di rete per l'instradamento / indirizzamento.
Gateway	è un dispositivo di rete che collega due reti informatiche di tipo diverso
Netmask	nell'ambito di una rete TCP/IP, è un parametro di configurazione che definisce la dimensione (intesa come intervallo di indirizzi) della sottorete IP, o subnet, a cui appartiene un host.
DNS	Domain Name System è un sistema utilizzato per assegnare nomi ai nodi della rete (es. www.unipr.it).
Mac Address	detto anche indirizzo fisico, indirizzo ethernet o indirizzo LAN, è un codice assegnato in modo univoco dal produttore ad ogni scheda di rete ethernet o wireless prodotta al mondo.
DHCP	Dynamic Host Configuration Protocol è un protocollo applicativo che permette ai dispositivi o terminali di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso, da una rete IP, la configurazione IP necessaria per stabilire una connessione e operare su una rete più ampia basata su Internet Protocol.
Rete GARR	rete italiana a banda ultralarga dedicata alla comunità dell'istruzione, della ricerca e della cultura.
Single sign on	autenticazione unica o identificazione unica è la proprietà di un sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato.

Premessa

L'Università degli Studi di Parma (d'ora in poi definita Ateneo) ritiene indispensabile l'adozione di tecnologie informatiche e telematiche per lo svolgimento delle proprie attività istituzionali e per il miglioramento costante dei servizi offerti all'utenza, e ritiene altresì che l'utilizzo della rete Internet sia un imprescindibile strumento per garantire la più ampia visibilità e diffusione delle informazioni relative alla propria attività istituzionale.
L'Ateneo deve adottare adeguati controlli per tutelare la riservatezza, l'integrità e la disponibilità dei dati secondo le buone pratiche e gli standard in materia di sicurezza delle informazioni, in ottemperanza agli obblighi normativi esistenti (leggi sul diritto d'autore, leggi sulla privacy *D.lgs 196/2003* aggiornato al *D.lgs 101/2018 - Codice in materia di protezione dei dati personali, Regolamento Europeo - Regolamento UE 2016/679 del Parlamento Europeo L. 119 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* pubblicato sulla GUUE del 04 maggio 2016 (di seguito GDPR), *D.lgs. 7 marzo 82/2005* e successive modifiche - *Codice dell'Amministrazione digitale*, *Circolare 18 aprile 2017, n.2/2017*, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni» *Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015*).

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi a principi di responsabilità, diligenza e correttezza espressi all'interno del ***Codice Etico*** ed essere finalizzato esclusivamente ad attività previste nel quadro dell'attività istituzionale, amministrativa, di didattica e di ricerca, l'Ateneo ha adottato una politica interna per l'attuazione e la diffusione di una cultura in materia di sicurezza informatica a tutela dell'**integrità**, della **disponibilità** e della **riservatezza delle informazioni**.

L'Ateneo eroga ai suoi utenti servizi attraverso risorse informatiche di vario tipo. Essi sono descritti all'interno del ***Catalogo dei servizi informatici***. Il presente regolamento definisce le condizioni di accesso e di utilizzo dei servizi e delle risorse informatiche dell'Ateneo; per gli aspetti specifici di alcuni servizi si rimanda ai relativi regolamenti.

1. Obiettivi

Il presente Regolamento ha i seguenti obiettivi:

- **prevenire**, ove possibile, comportamenti anche inconsapevoli che possano minacciare o compromettere la sicurezza nel trattamento dei dati, il rispetto della normativa sul diritto d'autore, e/o l'accesso stesso alle risorse dell'Ateneo;
- **codificare** le regole di comportamento da seguire per un corretto utilizzo degli strumenti e servizi onde evitare problemi, disservizi, costi aggiuntivi e rischi per la sicurezza dei dati e del patrimonio dell'Ateneo;
- **preservare** la sicurezza nell'accesso alla rete interna e alla rete Internet;
- **garantire** il rispetto delle leggi in materia di utilizzo delle risorse informatiche per l'elaborazione dei dati personali ai sensi del GDPR, Provvedimenti del Garante della Privacy collegati e normativa nazionale di settore;
- **informare** con chiarezza gli interessati sulle attività di monitoraggio e controllo;
- **diffondere** una cultura della sicurezza che concorra al conseguimento ed al mantenimento dei più alti livelli qualitativi dei servizi resi.

2. Ambito di applicazione

Il presente Regolamento si applica all'intero Ateneo, per tutte le sue sedi e riguarda tutti le risorse umane, fisiche e virtuali.
Questo Regolamento è destinato agli individui e al personale a vario titolo coinvolto nelle attività dell'Ateneo ed a tutti coloro che utilizzano i servizi ICT dell'Ateneo e definisce le politiche adottate a garanzia della sicurezza delle informazioni direttamente dall'Ateneo alle quali devono uniformarsi anche i fornitori/outsourcer di servizi/attività funzionali all'erogazione dei servizi ICT.

A mero titolo esemplificativo e non esaustivo, i soggetti interessati possono essere:

- Docenti (Professori Ordinari, Professori Associati, Ricercatori, Professori emeriti, Professori onorari);
- Personale Tecnico Amministrativo;
- Dottorandi;
- Borsisti di ricerca;
- Assegnisti di ricerca;
- Specializzandi;
- Studenti (studenti regolarmente iscritti in corsi di studio istituzionali. Tra i quali: studenti Erasmus, studenti iscritti a corsi interateneo);
- Collaboratori con cui intercorre un rapporto di lavoro formalizzato o di collaborazione a qualsiasi titolo a tempo determinato;
- Consulenti e fornitori;
- Spin-off e start-up;
- Società esterne;
- Ospiti.

TITOLO I
Sicurezza delle informazioni

1. Classificazione delle informazioni

L'Ateneo ha definito una specifica politica, vedi allegato ***Politica di Classificazione dei Dati***.

2. Condivisione delle informazioni

I dati e i documenti utilizzati nell'attività lavorativa devono essere condivisi secondo le modalità descritte nel documento *Politica di Classificazione dei Dati*. In particolare, i dati a cui è attribuito un livello di protezione superiore al *1-basso*, devono essere salvati e archiviati sugli strumenti designati dall'Ateneo (ad es.: cartelle di rete suddivise per area o competenza e strumenti di condivisione in cloud).
I dispositivi rimovibili (ad es.: chiavette e dischi esterni USB) devono essere utilizzati solo per necessità lavorative e devono essere forniti dall'Ateneo (non è possibile usare supporti personali). In particolare, i dispositivi rimovibili che contengono dati a cui è attribuito un livello di protezione superiore al *1-basso* devono implementare la cifratura in modo da non essere leggibili in caso di furto o smarrimento del supporto. I supporti devono essere custoditi con la massima cura per evitare furto o smarrimento.
La condivisione dei dati con soggetti esterni all'Ateneo è autorizzata solo nell'ambito dell'attività lavorativa e deve seguire standard, protocolli e canali che prevedano la cifratura. In generale tutti gli scambi di dati con l'esterno devono avvenire su canali cifrati per garantire la riservatezza dei dati, quindi reti VPN, connessioni HTTPS/TSL/SFTP, etc.
Non è consentito l'utilizzo di servizi personali di condivisione (ad es.: Google Drive, DropBox, WeTransfer, etc.) per il trattamento di dati nell'ambito delle attività lavorative.

3. Utilizzo della rete Internet

L'accesso e l'utilizzo alla rete Internet costituiscono parte integrante e fondamentale degli strumenti informatici che l'Ateneo mette a disposizione per lo svolgimento delle attività lavorative e non può in generale essere rivolto a fini personali.
L'Ateneo individua nella disponibilità e nella sicurezza delle connessioni di rete alcuni degli elementi fondamentali per garantire l'efficienza dei processi e la salvaguardia dei dati. Questo comporta la necessità di politiche e regolamentazioni che incoraggino un uso responsabile delle risorse condivise, e in particolare della rete Internet.
L'Ateneo regola il traffico consentito in ingresso e in uscita dalla rete di Ateneo e mediante tecnologie di filtro dei contenuti (vedi allegato ***Politica di filtro sul traffico di rete***) può preventivamente limitare o impedire l'accesso a servizi e/o contenuti che ritiene a suo insindacabile giudizio:

- illeciti;
- non appropriati;
- pericolosi per la sicurezza dei dati e delle persone;
- non pertinenti lo svolgimento dell'attività lavorativa.

Qualora risultassero non accessibili anche risorse che l'utente ritiene necessarie per finalità lavorative, egli può produrre una richiesta debitamente motivata all'Area Sistemi Informativi (d'ora innanzi ASI) al fine di revocare il blocco in via temporanea o definitiva.

4. Utilizzo della posta elettronica

Il profilo di posta elettronica di Ateneo è uno strumento di lavoro e l'utente è responsabile del suo corretto utilizzo secondo quanto disposto dal presente regolamento e dal ***Regolamento di utilizzo della Posta Elettronica di Ateneo*** secondo la normativa vigente. L'utilizzo a fini personali è vietato. L'utente è responsabile di:

- utilizzare il servizio di posta elettronica solo per le finalità istituzionali dell'Ateneo;
- non arrecare danni e/o pregiudizi all'Ateneo, a terzi o ad altri utenti;
- ispirarsi sempre a principi di diligenza, correttezza e buona fede, uniformandosi nei contenuti e nella forma dei messaggi ad adeguati standard di cortesia e buona condotta.

L'utente non può utilizzare la posta elettronica per inviare volutamente, anche tramite collegamenti o allegati in qualsiasi formato (ad es.: testo, foto, video, audio, etc.), messaggi che:

- possano danneggiare la reputazione e l'immagine dell'Ateneo o comprometterne le relazioni con soggetti terzi;
- siano diffamatori, osceni, pornografici, offensivi, tali da recare danno o che possano essere considerati fonte di molestie o discriminazione religiosa, sessuale, razziale, politica;
- contengano pubblicità non istituzionale, manifesta, occulta o comunicazioni commerciali private;
- possano infrangere la legislazione vigente, in particolare quella sui diritti d'autore;
- contengano malware o altri programmi dannosi oppure si configurino come spam messaggi indesiderati (noti come "spam").

L'utente è responsabile della corretta gestione delle credenziali di accesso al profilo di posta elettronica, come definito dal presente regolamento.

5. Documenti cartacei

Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o contenitori in dotazione alle unità operative. Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico. L'accesso agli archivi è consentito solo al personale espressamente autorizzato. Gli archivi devono essere chiusi a chiave, compatibilmente con le esigenze di servizio. Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali. Gli utenti sono tenuti a vigilare sull'accesso ai locali in cui operano da parte di personale non identificato o non autorizzato. Tutti i documenti cartacei di carattere amministrativo contenenti dati personali o dati dell'Ateneo ad accesso riservato devono essere smaltiti utilizzando gli strumenti distruggi-documenti in dotazione previa procedura autorizzatoria da parte della competente soprintendenza per i beni archivistici come previsto dalla normativa di riferimento.
Gli utenti devono utilizzare la stampante più vicina alla propria postazione di lavoro, ogni volta che sia possibile. I documenti stampati non devono essere lasciati incustoditi per evitare accessi non autorizzati ai dati, se possibile meglio privilegiare l'opzione di stampa in presenza avviata da un codice personale. Il riutilizzo di stampe come carta di riciclo è consentito solo quando i documenti contengono dati non personali e pubblici, in tutti gli altri casi le copie vanno smaltite utilizzando gli strumenti distruggi-documenti in dotazione. Le tempistiche di conservazione sono regolate da quanto disposto dal Manuale di Gestione del Protocollo e dal Manuale di Selezione e Prontuario di Scarto.

6. Controllo, monitoraggio e registrazione

L'Ateneo si riserva il diritto di controllare l'accesso, l'utilizzo e il funzionamento dei servizi ICT da esso erogati, sia tramite sistemi di monitoraggio automatico centralizzato, sia tramite agenti installati sulle postazioni, sia durante gli interventi di manutenzione; si riserva inoltre il diritto di mantenere registri delle attività (log) di vario tipo inerenti i servizi nel rispetto della normativa vigente di trattamento dei dati personali (vedi allegato ***Politica di gestione dei log***, che dettaglia le fonti da cui si raccolgono i log e le modalità di gestione)

Tali controlli sono finalizzati a:

- ottemperare alla normativa cogente in materia protezione dei dati e del diritto d'autore;
- rispondere ad eventuali richieste dell'autorità giudiziaria;
- garantire la sicurezza dei servizi anche tramite sistemi per la verifica delle intrusioni informatiche (IDS);
- verificare la corretta gestione dei flussi di dati e informazioni;
- implementare l'inventario delle risorse in rete e dei software utilizzati;
- elaborare statistiche d'uso, gestendo il dato in forma anonima, relative ai sistemi informatici;
- svolgere attività relative a modifiche tecniche/operative;
- verificare la corretta configurazione dei sistemi;
- raccogliere e preservare le evidenze forensi a supporto di ogni eventuale azione legale che coinvolga l'Ateneo;
- contrastare utilizzi impropri e/o illeciti e più in generale contrari alla politica di uso accettabile, al presente disciplinare ed alla normativa vigente;
- monitorare l'uso delle credenziali esposte.

È escluso ogni utilizzo dei dati raccolti per fini diversi da quelli sopra citati, in particolare per qualunque forma di controllo a distanza degli utenti.
L'accesso ai registri delle attività (log) è consentito solo al personale autorizzato e riguarda in primo luogo dati aggregati non riferibili a un singolo utente. L'accesso ai dati di utilizzo di un singolo utente, laddove necessario, avviene per giustificati motivi. In nessun caso sono ammessi controlli prolungati e costanti.
Alcune attività (ad es. amministratori di sistema) sono raccolte e gestite in adempimento alla normativa vigente.

7. Gestione degli Incidenti di sicurezza

Gli incidenti vengono tracciati su apposito registro secondo modalità previste nell'allegato ***Politica di gestione degli incidenti di sicurezza***.
Tutti gli utenti hanno l'obbligo di segnalare tempestivamente ogni anomalia nel funzionamento del sistema informativo di Ateneo o qualsiasi comportamento volontario o accidentale, anche di terzi esterni all'Ateneo, che possa esporre i dati oggetto del trattamento al rischio di furto, perdita o modifica non autorizzata. Nel caso si sospetti una compromissione degli strumenti informatici da parte di un malware o di un soggetto esterno all'Ateneo, questa deve essere segnalata prima possibile ai contatti inseriti in allegato.
Le misure di sicurezza preventive adottate dall'Ateneo e i comportamenti responsabili messi in atto dai collaboratori riducono la probabilità che si verifichi un incidente di sicurezza, ma non la

annullano, pertanto è molto importante che ogni situazione anomala venga gestita nel modo corretto, anche per mettere in condizione l'Ateneo di rispondere tempestivamente a tutti gli obblighi di legge in materia di protezione dei dati.
Un incidente di sicurezza non deve mai essere nascosto, ed è molto importante che in caso di sospetta compromissione di uno strumento di lavoro o delle credenziali di accesso personali, l'utente coinvolto si attenga a questo semplice protocollo:

- non spegnere per nessuna ragione il dispositivo (ad es.: PC, Smartphone, etc.);
- interrompere il collegamento alla rete dati (ad es. staccare il cavo di rete, disabilitare il WIFI. etc.);
- non cancellare niente dal dispositivo perché i dati raccolti possono essere fondamentali per l'analisi e la risoluzione dell'incidente;
- segnalare immediatamente l'anomalia come potenziale incidente di sicurezza e attenersi alle istruzioni che verranno impartite.

8. Limitazione dell'utilizzo delle risorse

A seguito della rilevazione di un incidente informatico e/o per rispondere a richieste delle Autorità Investigative e in considerazione della possibilità di dover rispondere ad eventuali obblighi legali di rispetto della catena di custodia volta a preservare evidenza di incidenti particolarmente gravi, l'ASI può:

- limitare o impedire l'uso del dispositivo (ad es.: esclusione dalla rete di Ateneo) o l'accesso ai servizi di Ateneo;
- chiedere la consegna del dispositivo per il tempo necessario a compiere le attività di analisi e risoluzione dell'incidente;
- imporre il ripristino sicuro e verificato dai tecnici ASI del dispositivo come condizione necessaria per l'accesso ai servizi di Ateneo.

TITOLO II
Gestione e utilizzo di dispositivi dell'Ateneo

1. Strumenti informatici

Le postazioni di lavoro informatiche e più in generale gli strumenti atti ad elaborare informazioni comprendono i dispositivi di proprietà dell'Ateneo, inclusi anche quelli acquistati tramite fondi di ricerca, assegnati al personale, quali, a titolo esemplificativo e non esaustivo:

a. personal computer da tavolo;
b. personal computer portatili;
c. thin-client e postazioni diskless;
d. virtual desktop;
e. tablet e dispositivi palmari;
f. smartphone e telefoni fissi;
g. server;
h. stampanti.

Ogni dispositivo, quando possibile, è inserito nel dominio Active Directory di Ateneo (on-premise o cloud), con profili predefiniti in base a ruolo e mansione dell'utente.

2. Gestione

La postazione di lavoro deve essere utilizzata solo per scopi istituzionali e su di essa devono essere conservati solo dati inerenti alle attività lavorative.
L'utilizzo degli strumenti dell'Ateneo deve essere sempre improntato ai principi di correttezza e liceità, in particolare è vietato modificare la configurazione hardware e/o software degli strumenti informatici concessi in uso, aggiungendo o rimuovendo componenti, rispetto allo standard definito e fornito dall'Ateneo oppure eludendo o compromettendo i meccanismi di protezione.
È vietato:

- cancellare dolosamente dati dell'Ateneo o copiarli su supporti personali;
- agire deliberatamente per degradare l'operatività dei sistemi e della rete dell'Ateneo e per impedirne l'uso da parte di altri utenti;
- effettuare trasferimenti di informazioni (ad es. software, dati, etc.) e di documenti concernenti proprietà intellettuale, se non per lo svolgimento delle proprie funzioni istituzionali;
- installare, eseguire o diffondere su qualunque computer e sulla rete programmi che possano danneggiare i sistemi o determinare un accesso non autorizzato ai dati (ad es. malware, etc.);
- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare dati di altri utenti;
- utilizzare software che mettano a rischio la sicurezza dei sistemi e la protezione dei dati;
- installare software privo di regolare licenza d'uso in corso di validità;
- utilizzare strumenti dell'Ateneo per la conservazione o la condivisione di materiale per il quale si configuri la violazione della normativa a protezione del diritto d'autore, nonché di materiale pornografico o in qualsiasi modo illecito o lesivo della dignità umana.

Il rispetto delle suddette prescrizioni contribuisce alla prevenzione dei reati informatici.

Qualora sia necessario, gli utenti possono richiedere, previa verifica da parte del proprio responsabile, l'aggiornamento della propria configurazione rivolgendosi ad ASI.

Alla cessazione del rapporto di lavoro oppure nel caso in cui non sussistano più le condizioni per le quali gli utenti li avevano ricevuti, inclusi i casi di variazione di mansione e/o passaggio ad un'altra Unità/Area, questi devono restituire gli strumenti informatici in loro possesso integri e in buono stato di conservazione.

2.1 Salvataggio dei dati

Le postazioni inserite nel dominio di Ateneo devono conservare i dati nello spazio disco condiviso messo a disposizione dall'Ateneo e gestito dall'ASI (ad es. cartelle condivise, OneDrive, Sharepoint) in quanto sottoposto alle opportune procedure che garantiscono la disponibilità del dato.
Per le postazioni che dovessero temporaneamente trovarsi ancora fuori dominio sarà cura e responsabilità unica dell'utente provvedere ad effettuare copie di salvataggio dei dati tenendo conto di quanto prevedono la normativa vigente e la *Politica di Classificazione dei Dati*.

2.2 Presidio della postazione

Il PC deve essere spento ogni sera prima di lasciare gli uffici e ogni qual volta ci sia la necessità di allontanarsi dal posto di lavoro, anche quando ci si trova per qualunque motivo (missione, smart-working, telelavoro etc.) in locali esterni all'Ateneo, deve essere attivata la protezione tramite password (screen saver con password o blocco del computer con password). Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

2.3 Strumenti di sicurezza

Tutti i personal computer fissi e mobili sono dotati di strumenti di aggiornamento automatico dei sistemi operativi, di difesa da malware e di monitoraggio delle anomalie: l'utente non deve in nessun modo intralciare o inibire il funzionamento di questi strumenti, limitandosi a segnalare tempestivamente qualsiasi tipo di problema all'helpdesk informatico.
L'Ateneo si può avvalere di sistemi di gestione centralizzata dei personal computer fissi e mobili al fine di:

- attivare procedure di autenticazione aggiuntive;
- imporre il rispetto delle configurazioni prestabilite e inibirne la modifica;
- inventariare automaticamente l'hardware e il software;
- definire adeguate politiche di back-up dei dati;
- aggiornare automaticamente i sistemi operativi e il software;
- attivare procedure di cancellazione remota da utilizzare in caso di smarrimento/furto del dispositivo;
- cifrare automaticamente i dati;
- inibire l'installazione di applicazioni indesiderate;
- filtrare i contenuti in ingresso alla rete dell'Ateneo inibendo preventivamente quelli ritenuti non appropriati o non necessari allo svolgimento delle attività lavorative.

Ogni strumento fornito dall'Ateneo può inoltre essere dotato di software di gestione e monitoraggio da remoto. Il personale ASI utilizza questi strumenti per collegarsi alle singole postazioni al fine di garantire l'assistenza tecnica. L'intervento da remoto viene effettuato esclusivamente su chiamata dell'utente o a seguito della rilevazione di problematiche tecniche. In quest'ultimo caso verrà data comunicazione della necessità dell'intervento all'utente che dovrà esplicitamente autorizzare il personale di supporto all'esecuzione dell'attività.

2.4 Furto o smarrimento

I PC portatili devono essere custoditi in modo da minimizzare il rischio di furto e smarrimento, soprattutto quando si trovano all'esterno dell'Ateneo. I supporti di memoria dei pc portatili sono cifrati in modo che nessuno possa effettuare un accesso non autorizzato ai dati anche se viene in possesso fisico dei dispositivi. Questo comporta generalmente che l'utente debba inserire all'avvio del pc un codice di sblocco fornito dall'Ateneo, che deve rimanere segreto e deve essere gestito secondo le linee guida previste per le credenziali di accesso definite dal presente regolamento.
In caso di furto o smarrimento di un qualsiasi dispositivo (fisso o mobile), gli utenti sono tenuti a:

- notificare l'accaduto all'helpdesk informatico, richiedendo contestualmente il blocco dei profili o della SIM se applicabile e, qualora il dispositivo contenga dati personali, scrivere anche all'indirizzo di comunicazione dei databreach (vedi dettaglio contatti in allegato);
- sporgere denuncia alle forze dell'ordine;
- richiedere ad ASI una nuova dotazione allegando la denuncia effettuata alle forze dell'ordine.

3. Utilizzo di strumenti non forniti dall'Ateneo all'interno delle sedi di Ateneo

Per quanto riguarda l'utilizzo di strumenti non forniti dall'Ateneo (anche il solo collegamento alla rete di Ateneo è un utilizzo):

- è consentito collegarsi alla rete WiFi di Ateneo tramite accesso autenticato con credenziali di Ateneo;
- è consentito collegarsi alla rete cablata secondo quanto disposto dal TITOLO III art. Collegamento dei dispositivi alla rete.

4. Telelavoro o lavoro agile

Il telelavoro e il lavoro agile (smart-working) vengono svolti solo con dispositivi di proprietà dell'Ateneo che rispettano le indicazioni e le misure di sicurezza previste in questo Regolamento.
Il precedente capo non si applica in situazioni emergenziali debitamente codificate da disposizioni di legge.

4.1. Protezione da furto e smarrimento dei dati presenti sui dispositivi

Considerato che l'ambiente di lavoro non è quello usuale dell'ufficio e potrebbero esserci maggiori opportunità di accesso non autorizzato ai dati da parte di soggetti esterni all'Ateneo, valgono senza eccezioni tutte le disposizioni descritte nel presente regolamento (vedi soprattutto paragrafo 2).

4.2. Protezione dei dati in transito sulla rete

Tutte le comunicazioni di pertinenza lavorativa devono avvenire su canali di comunicazione cifrata, che utilizzano quindi protocolli adeguati a garantire la riservatezza dei dati. L'Ateneo definisce e comunica agli interessati quali strumenti sono idonei per le finalità di scambio dati, videoconferenza, etc. Le indicazioni fornite dall'Ateneo sono vincolanti e quindi è vietato utilizzare strumenti diversi che potrebbero non avere gli standard di sicurezza richiesti.

L'accesso remoto alla rete di Ateneo viene garantito attraverso l'uso di un canale di comunicazione cifrato VPN (Virtual Private Network), che viene attivato mediante l'uso di specifico software (client VPN) installato sui dispositivi abilitati. L'utente utilizzerà le credenziali personali di accesso da gestire secondo le disposizioni del presente regolamento. L'Ateneo potrebbe modificare le modalità tecniche di collegamento privilegiando altre soluzioni equivalenti sotto il profilo della sicurezza come l'utilizzo di desktop virtuali forniti dall'Ateneo.

Se il collegamento verso la rete Internet avviene attraverso la rete WiFi privata dell'utente (ad esempio la connessione di casa), questi deve assicurarsi che il livello di sicurezza della rete sia compatibile con i requisiti dell'Ateneo seguendo, ad esempio, queste indicazioni:

- cambiare la password di default accesso al WIFI;
- disattivare, quando possibile, l'accesso amministrativo al router WiFi da una rete esterna;
- verificare che il pc dell'Ateneo non condivida risorse con nessun altro dispositivo attestato sulla rete casalinga;
- impedire al PC dell'Ateneo di accedere ad altri dispositivi di memorizzazione della rete casalinga (NAS, dischi esterni, etc.).

Nel caso vengano utilizzate reti pubbliche (es.: WiFi dell'albergo, aeroporto, biblioteche etc.) è indispensabile utilizzare la VPN per accedere ai servizi dell'Ateneo che prevedano l'autenticazione.
I collegamenti VPN sono monitorati per motivi di sicurezza e conformità normativa, in particolare in relazione agli accessi dei profili privilegiati. Tutte le modalità di monitoraggio e controllo dei sistemi, così come l'assistenza remota sono attivi anche in smart working.

5. Assistenza

L'assistenza viene fornita conformemente a quanto previsto nel Catalogo dei servizi dell'Area Sistemi Informativi.

6. Smartphone e Tablet

Qualora venisse assegnato dall'Ateneo un cellulare/smartphone/tablet all'utente, quest'ultimo sarà responsabile della custodia e del suo corretto utilizzo. Oltre che per l'uso dei consueti strumenti lavorativi (es.: posta elettronica, gestione documentale, etc.), lo smartphone può essere configurato dall'Ateneo come generatore di codici per l'accesso a sistemi o applicativi che richiedono l'autenticazione a due fattori, pertanto riveste un ruolo centrale nelle strategie di gestione della sicurezza delle informazioni e deve essere protetto in misura adeguata.
I supporti di memoria dei dispositivi mobili sono cifrati e ogni dispositivo verrà consegnato con un codice (PIN) di sblocco per proteggerlo da accessi non autorizzati in caso di furto o smarrimento: il codice PIN non può essere tolto per nessun motivo.

L'Ateneo può avvalersi di sistemi di gestione centralizzata dei dispositivi mobili come già definito nel TITOLO II art. 2.3 Strumenti di sicurezza per le postazioni di lavoro fisse e mobili.

Eventuali regole specifiche per l'utilizzo dei dispositivi mobili potranno essere esplicitate nella modulistica di assegnazione degli strumenti agli utenti. L'Ateneo non è in ogni caso responsabile per la perdita di dati e documenti personali dell'utente conservati sul dispositivo.

TITOLO III
RETE DI ATENEO

1. Accesso

L'Università di Parma considera la Rete Dati di Ateneo un elemento strategico e fondamentale per il perseguimento dei propri fini istituzionali e, quindi, ne promuove lo sviluppo, il buon funzionamento e la sicurezza. Ne favorisce, quindi, l'accesso agli utenti (docenti, PTA, studenti, …) con le tecnologie disponibili, secondo profili differenziati adottando nel contempo tutte le misure necessarie per mitigare il rischio.
Il servizio di accesso alla rete interna e ad Internet deve essere utilizzato a fini istituzionali, rispettando le regole di comportamento previste nel presente regolamento e della AUP (Acceptable Use Policy) del Consortium GARR. Il regolamento, in particolare, è da ritenersi sempre applicabile a prescindere dalla tipologia di dispositivo utilizzato per l'accesso alla rete di Ateneo.
Al fine di controllare e gestire la sicurezza della rete di Ateneo, l'accesso alla rete cablata potrà avvenire tramite richiesta di credenziali e potranno essere applicate limitazioni alla navigazione (es.: blocco verso URL che conducono a contenuti pericolosi o malevoli).

2. Collegamento dei dispositivi

Per il primo collegamento di un qualunque dispositivo alla rete è necessario inoltrare, tramite l'helpdesk informatico, una richiesta all'ASI che provvederà a rilasciare le informazioni necessarie (es.: Indirizzo IP, Gateway, Netmask, DNS, …) secondo i criteri di autorizzazione in vigore.
Il dispositivo, quindi, è inventariato come "risorsa attiva" e la coppia indirizzo IP/MAC ADDRESS viene registrata e associata all'utente che ha ne ha fatto richiesta (sia che l'indirizzo sia statico o erogato in maniera dinamica, per esempio con DHCP).
Per poter gestire la sicurezza del dispositivo e della rete di Ateneo, l'ASI installerà agenti software a basso impatto che forniranno centralmente informazioni sulle vulnerabilità presenti sul dispositivo, sulla presenza di software malevolo, non autorizzato o altre informazioni di carattere tecnico utili alla gestione del sistema di sicurezza di Ateneo.
Tali agenti non raccolgono dati finalizzati al monitoraggio dell'attività dell'utente e non devono essere rimossi o disattivati.

3. Connessione di laboratori informatici e postazioni pubbliche

1. La connessione alla rete di Ateneo di postazioni dei laboratori informatici, postazioni pubbliche o altre tipologie di aree attrezzate avviene attraverso l'infrastruttura di virtualizzazione dei desktop di Ateneo
2. All'interno delle strutture di cui al punto 1 è vietato disconnettere i dispositivi presenti dalla rete cablata e/o connettere alla rete cablata dispositivi diversi da quelli installati ed autorizzati dall'Ateneo.

4. Richieste di assegnazione di risorse e servizi accessibili dall'esterno

Chiunque ne abbia facoltà, può richiedere per finalità istituzionali (compatibili con le AUP del GARR) l'assegnazione di adeguate risorse e servizi di comunicazione su IP definiti facendone esplicita richiesta adeguatamente motivata che sarà valutata ed eventualmente approvata dal Rettore o suo delegato.
Le richieste di apertura di porte/protocolli di comunicazione saranno valutate rispetto a criteri di sicurezza in modo da minimizzare il rischio.

Gli assegnatari hanno la responsabilità di mantenere i sistemi e gli applicativi aggiornati e correttamente configurati in modo da non comportare rischi alla sicurezza delle informazioni e devono attenersi alle indicazioni dell'ASI riguardo ad eventuali configurazioni e installazione di strumenti necessari per i controlli di sicurezza (es.: agenti, sonde …).
A questo proposito ASI svolge verifiche periodiche sulle vulnerabilità e segnala le criticità da correggere nei tempi concordati, pena la decadenza dei privilegi e il blocco dei servizi assegnati.
ASI ha inoltre facoltà di monitoraggio della rete, dei sistemi, dei servizi e degli applicativi al fine di evidenziare anomalie e incidenti di sicurezza che saranno gestiti secondo le politiche in vigore.
La gestione del traffico in ingresso e in uscita dalla rete di Ateneo prevede la negazione implicita di ogni flusso di comunicazione da e verso l'esterno che non sia esplicitamente autorizzato. Questo permette di controllare sia i soggetti che possono comunicare con l'esterno che i servizi che la rete di Ateneo espone sulla rete pubblica Internet o verso partner, fornitori, utenti dei servizi, ricercatori, etc.
I sistemi che offrono servizi verso reti pubbliche o private esterne devono essere installati su infrastrutture dedicate e gestite centralmente facilitando così la gestione della sicurezza della rete e l'adeguatezza dei controlli applicati ai sistemi e agli applicativi.

TITOLO IV
Profilazione degli utenti

1. Identità digitale di Ateneo

L'identità digitale è costituita dalle informazioni relative ad un utente, denominate attributi, utilizzate per rappresentarne l'identità, lo stato, la forma giuridica o altre caratteristiche peculiari ed è verificata attraverso un sistema di identificazione e autenticazione informatica.
Le identità digitali di Ateneo sono costituite da nome utente, password dati personali, informazioni sulla carriera e altri dati a uso esclusivo dei sistemi e delle procedure informatiche. L'identità digitale è strumentale all'accesso a uno o più servizi telematici.
L'Ateneo favorisce la partecipazione alle Federazioni di Autenticazione previste dall'ordinamento nazionale (SPID) o in uso sulle reti dell'università e della ricerca a livello nazionale, europeo e mondiale, quali ad esempio Eduroam, IDEM, che operano in una logica di identità federate.

2. Titolari di identità digitali

I titolari delle identità digitali di Ateneo sono tutti i soggetti che devono fruire di un servizio dell'ateneo stesso.

3. Responsabilità dei titolari di identità digitale

1. Ciascun titolare di identità digitale, in fase di utilizzo dei servizi, non deve:
    - Violare la privacy di altri Utenti o dell'integrità di dati non di sua pertinenza, siano essi personali o meno;
    - Compromettere l'integrità dei sistemi o dei servizi;
    - Consumare risorse in misura tale da compromettere l'efficienza di altri servizi;
    - Compiere, agevolare o supportare indirettamente atti di criminalità informatica contro e/o attraverso le infrastrutture e le risorse dell'Ateneo;
    - Sfruttare i servizi dell'Ateneo per accedere senza autorizzazione a risorse dell'Ateneo o di terze parti;
    - Condividere con terzi non autorizzati l'accesso a servizi dell'Ateneo;
    - Usare false identità, l'anonimato o servirsi di risorse che consentono anche parzialmente di restare anonimi;
    - Violare gli obblighi contrattualmente assunti dall'Università per la realizzazione e la gestione della Rete Interna, particolarmente trasferendo e rendendo disponibile materiale che violi la normativa vigente ed in particolare le norme sulla proprietà intellettuale, le licenze d'uso di software e i regolamenti dei fornitori di connettività di rete (GARR);
    - Svolgere attività che causino malfunzionamento, diminuiscano la regolare operatività, distraggano risorse (persone, capacità, potenza di elaborazione), danneggino o restringano l'utilizzabilità dei servizi e delle risorse;
    - Violare la sicurezza di archivi e banche dati, compiere trasferimenti non autorizzati di informazioni (es.: software, basi dati, etc.), intercettare, tentare d'intercettare o accedere a dati in transito sulla Rete, dei quali non si è destinatari specifici;
    - Compiere o tentare di compiere le seguenti azioni: distruggere, intercettare, accedere senza autorizzazione ai dati di altri utenti o di terzi, usare, intercettare o diffondere password o codici d'accesso o chiavi crittografiche di altri utenti o di terzi, e in generale commettere attività che violino la riservatezza di altri utenti o di terzi, così come tutelata dalle norme civili, penali e amministrative applicabili;

- collegare apparecchiature alle infrastrutture di rete senza l'autorizzazione dell'ASI, inclusi i dispositivi personali;
- creare o diffondere immagini, dati o altro materiale potenzialmente offensivo, diffamatorio, o dal contenuto osceno;
- porre in essere attività che danneggiano l'immagine e il buon nome dell'Ateneo;
- utilizzare i servizi e le risorse informatiche di Ateneo a scopi commerciali e per propaganda politica o elettorale, tranne nei casi specificatamente autorizzati.

2. I servizi e le risorse informatiche erogati in collaborazione con soggetti esterni all'Ateneo sono soggetti a condizioni e termini di servizio stabiliti con i relativi fornitori. In caso di fruizione di un servizio in collaborazione con aziende esterne, l'utente accetta i termini d'uso nel momento in cui accede al servizio. L'Ateneo rende disponibili i riferimenti alle condizioni e termini di servizio nell'allegato A del presente regolamento oppure al momento del primo accesso al servizio.

4. Ciclo di vita delle credenziali di accesso al profilo

Le credenziali di accesso ad ogni profilo vengono create, disattivate, sospese e cancellate per le diverse categorie di utenti secondo gli schemi contenuti nell'allegato ***Ciclo di vita identità digitale***.

5. Autenticazione

Le modalità di autenticazione necessarie per l'utilizzo dei servizi sono indicate nel Catalogo dei Servizi (di seguito indicato come CdS). Si distinguono servizi che non richiedono autenticazione, servizi accessibili tramite le Credenziali di Autenticazione Centralizzata e servizi accessibili tramite credenziali specifiche del servizio.
Secondo quanto previsto dall'art. 64 del CAD l'accesso ai servizi di Ateneo dovrà essere consentito attraverso l'utilizzo di credenziali SPID.

6. Credenziali di Autenticazione Centralizzata

Le Credenziali di Autenticazione Centralizzata (rif. § 2.5 del CdS) sono il sistema di autenticazione principale per i servizi informatici dell'Ateneo. Le credenziali sono costituite da un identificativo (detto anche username o user id) e da una password. L'identificativo generalmente coincide con l'indirizzo mail universitario dell'utente, ma per alcune categorie di utenti può essere rappresentato da un codice numerico o essere valorizzato con un indirizzo email privato dell'utente. L'identificativo può essere modificato nel corso del rapporto dell'utente con l'Ateneo (ad esempio passaggio da studente a dipendente), ma viene mantenuto un rapporto univoco fra le Credenziali di Autenticazione Centralizzata e l'identità digitale dell'utente nel sistema informativo dell'Università.

6.1. Politica delle password

La password deve rispettare i criteri di robustezza e sicurezza indicati nell'allegato *Politica delle Password*.

6.2. Rilascio, sospensione e revoca delle Credenziali

Le credenziali, a seconda della categoria dell'utente, vengono rilasciate d'ufficio o previa registrazione. Le credenziali possono venire sospese, ad esempio per motivi di sicurezza nel caso se ne ipotizzi la compromissione.

6.3. Norme di utilizzo delle credenziali

Le credenziali sono strettamente personali, l'utente è tenuto a conservarle con diligenza avendo cura che non vengano utilizzate in modo improprio. La cessione a terzi delle proprie credenziali costituisce violazione del presente regolamento.
Al di fuori dei servizi compresi nella gestione con single sign on, l'utente deve scegliere password differenti per ogni sistema o applicativo a cui ha accesso, compresi eventuali servizi di terze parti a cui deve registrarsi con un profilo di posta elettronica fornito dall'Ateneo. Le credenziali non devono mai essere riutilizzate.
L'Ateneo può stabilire che l'accesso a determinati dati comporti un rischio più elevato e richieda pertanto un livello di sicurezza superiore: in questo caso potrebbe essere obbligatorio l'uso di sistemi di autenticazione a 2 o più fattori che comportano l'inserimento di un codice temporaneo generato da una applicazione mobile o da un dispositivo dedicato. Agli utenti interessati verranno fornitele istruzioni operative per un corretto utilizzo.
Tutte le credenziali sono strettamente personali e ogni utente è responsabile della loro custodia e riservatezza. Le politiche di Ateneo richiedono una scadenza periodica delle credenziali di accesso; l'utente verrà avvisato in modo automatico della necessità di scegliere una nuova password, rispettando sempre i criteri definiti in precedenza.
In caso non sia possibile implementare una procedura di cambio password automatica per determinati sistemi o applicativi, sarà cura dell'Ateneo definire una procedura manuale a cui fare riferimento.

Nel caso si sospetti che la propria password abbia perso la caratteristica della segretezza si deve procedere ad una modifica immediata della stessa, dandone comunicazione all'helpdesk informatico. Analogamente, qualora l'utente venga a conoscenza di credenziali violate di un altro utente, è tenuto a notificarlo immediatamente con le stesse modalità.

7. Credenziali locali

Per i servizi non integrabili nel sistema di autenticazione centralizzata è previsto l'uso di credenziali locali rilasciate dalla struttura incaricata dell'erogazione del servizio.
Nel caso di sistemi di credenziali basati su codice identificativo e password, la password dovrà essere gestita con criteri allineati alla *Politica delle Password*.

8. Abilitazione all'utilizzo dei servizi

L'utilizzo dei servizi che richiedono autenticazione è subordinato, oltre che al possesso delle credenziali di autenticazione, all'abilitazione delle stesse per il servizio in questione. L'Università adotta una politica di abilitazione basata su ruoli e profili di accesso: per ogni servizio sono individuati diversi profili di accesso, ad ogni ruolo sono assegnati uno o più profili di accesso per i vari servizi e ogni utente è inquadrato in uno o più ruoli.
Ogni utente è associato almeno ad un ruolo base corrispondente alla categoria di appartenenza e, eventualmente ad altri ruoli aggiuntivi in base, principalmente, alla categoria dell'utente, alla struttura di afferenza e alle attività di competenza.
I criteri di appartenenza ai ruoli aggiuntivi e i profili di accesso da associare ai vari ruoli vengono stabiliti dalle aree dirigenziali e dai dipartimenti tramite loro incaricati, in coordinamento con il personale incaricato della gestione operativa dei sistemi di abilitazione che si dovrà occupare fra l'altro del mantenimento di un catalogo dei ruoli e dei profili di accesso esistenti e della verifica periodica della corretta associazione degli utenti ai ruoli e dei profili di accesso corrispondenti ad

ogni ruolo. La verifica viene svolta con maggior puntualità e frequenza per i ruoli che consentono l'accesso a informazioni sensibili e/o riservate.
L'associazione ad un ruolo può avvenire d'ufficio o in base ad una richiesta effettuata a seconda dei casi dall'utente stesso o da un responsabile (ad esempio il responsabile della struttura di afferenza o il docente responsabile).
Per motivi di sicurezza e riservatezza:

- le abilitazioni all'utilizzo dei servizi sono strettamente personali, è vietato utilizzare le proprie abilitazioni per consentire ad altri utenti o a terzi l'utilizzo dei servizi con i propri privilegi di accesso;
- ad ogni ruolo vengono assegnati i profili di accesso minimi necessari a svolgere le attività di competenza degli utenti assegnati a quel ruolo;
- è responsabilità degli utenti segnalare con celerità eventuali errori dell'assegnazione dei privilegi ai gestori delle abilitazioni;
- i privilegi possono essere sospesi temporaneamente, previa comunicazione agli utenti interessati, in caso di abusi nell'utilizzo dei servizi o per altre giustificate necessità tecniche o di altro tipo;
- i ruoli vengono revocati all'utente quando non sono più in essere le condizioni per le quali il ruolo gli era stato assegnato.

L'assegnazione di un ruolo comporta la contemporanea attivazione dei privilegi di accesso previsti per quel ruolo sui vari servizi e la revoca di un ruolo comporta la rimozione dei privilegi di accesso. Per alcuni servizi è previsto che i privilegi di accesso non vengano revocati immediatamente, ma dopo un periodo di tempo prefissato indicato nel CdS o nell'allegato Ciclo di vita Identità Digitale del presente regolamento o in un apposito articolo di un eventuale regolamento specifico del servizio.

Allegati e riferimenti

Sezione A - Termini e condizioni di servizi di terze parti

- GARR – acceptable use policy AUP

Sezione B (contatti)

HELPDESK IT
Email: helpdesk.informatico@unipr.it
Telefono: +39.0521.90.6789

SEGNALAZIONE DATA BREACH
Email: databreach@unipr.it

DATA PROTECTION OFFICER
Email: dpo@unipr.it

Sezione C - Politiche e procedure di Ateneo

1. Politica di Classificazione dei Dati
2. Politica di filtro sul traffico di rete
3. Politica di Gestione dei log
4. Politica delle Password
5. Politica di Gestione degli Incidenti di Sicurezza
6. Ciclo di vita Identità Digitale
7. Regolamento di utilizzo della Posta Elettronica di Ateneo
8. Codice etico
9. Catalogo dei servizi informatici