UNIVERSITÀ
di VERONA

LINEE GUIDA SULL'UTILIZZO DI STRUMENTI E SERVIZI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA AI SENSI DELLA NORMATIVA SU SICUREZZA INFORMATICA E PROTEZIONE DEI DATI PERSONALI

Disposizioni per il corretto utilizzo degli strumenti e servizi informatici di Internet e della Posta Elettronica di Ateneo, per la sicurezza dei dati personali e delle informazioni redatto anche ai sensi del "Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (da ora in poi GDPR) e del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007)

Per il corpo docente e ricercatore sono previste particolari deroghe evidenziate con (*) nel titolo del paragrafo.

Al fine esclusivo di consentire lo svolgimento di attività di ricerca, con l'autonomia costituzionalmente garantita, è previsto che il personale docente e ricercatore, come i collaboratori che agiscano sotto la loro diretta responsabilità, possano derogare parzialmente ai divieti di cui agli articoli e ai paragrafi successivi, notificando le motivazioni al Direttore di Dipartimento e alla Direzione competente dei Sistemi Informativi, i quali potranno rispondere con diniego motivato alle richieste In ogni caso non sono derogabili disposizioni che direttamente o indirettamente modifichino il livello di sicurezza dei device del soggetto connessi alla rete.

Approvato dal Senato Accademico del 26 Luglio 2022

UNIVERSITÀ di VERONA

INDICE

1. Disposizioni generali

1.1 Definizioni

Apparecchiatura o dispositivo o device: qualsiasi computer (workstation o laptop) smartphone, tablet o altro tipo di dispositivo elettronico (comprese chiavette usb, hard disk, smart card o altri sistemi di memorizzazione o di gestione dei dati).

Ateneo / **Università:** Università degli Studi di Verona.

Autorizzato al trattamento o Soggetto autorizzato: ogni docente, ricercatore, dipendente, studente, collaboratore o fornitore, ed ogni altra persona fisica che sotto il controllo dell'Ateneo, nell'ambito dell'attività assegnatagli, tratta dati di nella disponibilità dell'Ateneo stesso.

Cessati: ogni "soggetto" che non ha più lo status di soggetto autorizzato.

Collaboratore: lavoratore/lavoratrice che presta la propria attività lavorativa senza vincolo di subordinazione con l'Ateneo.

Dipendente / **personale**: personale dell'Ateneo assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Disciplinare: il presente documento, recante la disciplina per l'utilizzo degli strumenti informatici, di internet e della posta elettronica.

Fornitore: persona fisica o giuridica (ente / azienda, titolare di ditta individuale, libero professionista) che approvvigiona di beni e servizi l'Ateneo.

GDPR: Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati.

Grazia: All'interruzione del rapporto, agli studenti, al personale docente, ricercatore e tecnico amministrativo viene concesso un periodo ulteriore di tempo, che prevede la conservazione della casella di posta elettronica, l'accesso ad Internet tramite rete cablata e Wi-Fi, i servizi ad essa correlati come la VPN e l'accesso a riviste e banche dati elettroniche oltre ai privilegi necessari per l'accesso. Tale status si definisce "di Grazia",

NDA: *Non Disclosure Agreement*, ovvero accordo di non divulgazione che designa informazioni confidenziali che le parti si impegnano a mantenere segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Studente: soggetto che risulta regolarmente iscritto ad un corso di laurea, di laurea magistrale, di specializzazione, di dottorato, di perfezionamento scientifico e di alta formazione permanente dell'Ateneo.

1.2 Premessa

L'ambito lavorativo porta il nostro Ateneo a gestire una serie di "**informazioni**", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del GDPR, "**dati personali**" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Ateneo adotti una serie di adeguate misure tecniche ed organizzative atte a proteggere tali dati.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "**informazioni riservate**", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'Ateneo è chiamato a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio di Ateneo.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "**dati**" deve intendersi l'insieme più ampio di informazioni di cui un **soggetto autorizzato** (dipendente, collaboratore, tirocinante, ...) può venire a

conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, l'Ateneo tratta "**dati cartacei**" ovvero informazioni su supporto cartaceo e "**dati digitali**" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui il soggetto autorizzato viene a conoscenza nell'ambito della propria attività lavorativa, può essere trattato entro il solo perimetro di trattamento specifico e consentito al soggetto. Nell'utilizzo di strumenti informatici generalmente distribuiti ed interconnessi per lo svolgimento di attività, con particolare riguardo all'accesso alla rete internet da device d'Ateneo, espone l'Università a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'Ateneo stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'Ateneo adotta il presente Disciplinare per evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature di Ateneo.

Il presente Disciplinare si applica ai **soggetti autorizzati** ad operare con dati e servizi dell'Ateneo ed è redatto in conformità alle seguenti fonti normative, regolamentari, linee guida e strumenti di soft law:

- Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati" (da ora in poi GDPR);
- Provvedimento del Garante per la protezione dei dati personali (Deliberazione n. 13 del 1/3/2007 - pubblicata sulla GU n. 58 del 10 marzo 2007);
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008;
- Agenzia per l'Italia Digitale - CIRCOLARE 18 aprile 2017, n. 2/2017 - Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»;
- Standard ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti).
- Acceptable Use Policy del GAAR (Regole di utilizzo della rete)

Una gestione dei dati cartacei, un uso di apparecchiature di Ateneo nonché dei servizi di internet e di posta elettronica difforme dalle regole contenute nel presente Disciplinare espone l'Ateneo ad una maggiore minaccia di accessi non autorizzati ai dati e/o al sistema informatico di Ateneo, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata a tutti i soggetti interessati.

1.3 Classificazione delle informazioni

Il Responsabile della struttura di afferenza del personale interessato deve approvare l'attribuzione di questa classificazione su insiemi di informazioni.

Informazioni pubbliche (open)

Tipo:	Informazioni che possono essere distribuite a chiunque senza causare danno all'organizzazione, ai dipendenti o agli stakeholders.

	I documenti in questa categoria possono essere comunicati al pubblico o a persone esterne all'organizzazione
Esempio:	Atti soggetti a pubblicazione obbligatoria, rendicontazioni, comunicazioni a studenti e dipendenti, comunicazioni al territorio, comunicati stampa, etc.
Responsabilità utilizzatore	Nessuna
Duplicazione	Senza vincoli
Distribuzione	Senza vincoli
Distruzione e riciclaggio	Senza vincoli
Etichetta:	Nessuna

Informazioni con accesso ristretto

Tipo:	Informazioni che possono essere divulgate ad un gruppo ristretto di soggetti interni / esterni all'Ateneo.
Esempio:	Documentazione di progetto – gara – concorso – procedura senza evidenza pubblica, archiviata e resa disponibile a ristretti gruppi di soggetti esterni o a utenti autorizzati.
Responsabilità utilizzatore	Responsabile del procedimento: responsabile di verificare che la distribuzione delle informazioni confidenziali sia limitata ai casi di effettiva necessità; Operatore: responsabile di seguire le istruzioni del Responsabile del procedimento.
Duplicazione	Come stabilito nell'ambito del procedimento interessato e della normativa / regolamenti di riferimento.
Distribuzione	Come stabilito nell'ambito del procedimento interessato e della normativa / regolamenti di riferimento.
Distruzione e riciclaggio	Come stabilito nell'ambito del procedimento interessato e della normativa / regolamenti di riferimento.
Etichetta:	Riservato o Interno

Informazioni confidenziali

Tipo:	Informazioni confidenziali o di valore, sia personali che sotto brevetto. Non devono assolutamente essere divulgate all'esterno dell'organizzazione senza l'esplicito permesso del responsabile della struttura d'afferenza.
Esempio:	Password, codici PIN, certificati di firma digitale, informazioni personali (non necessarie per la stipula di atti, altre informazioni altamente confidenziali o di valore.
Responsabilità utilizzatore	Responsabile del procedimento: responsabile di verificare che la distribuzione delle informazioni confidenziali sia limitata ai casi di effettiva necessità;

	Operatore: responsabile di seguire le istruzioni del Responsabile del procedimento.
Duplicazione	Come stabilito nell'ambito del procedimento interessato e della normativa / regolamenti di riferimento.
Distribuzione	Come stabilito nell'ambito del procedimento interessato e della normativa / regolamenti di riferimento.
Distruzione e riciclaggio	Come stabilito nell'ambito del procedimento interessato e della normativa / regolamenti di riferimento.
Etichetta:	Confidenziale

1.4 Uso degli strumenti e dei Servizi Informatici

All'inizio del rapporto con l'Ateneo, si è di norma autorizzati all'uso dei vari servizi e device di Ateneo, di internet e della posta elettronica in relazione alla propria mansione e ambito di trattamento. Ciò fino al termine del rapporto di lavoro a meno di prolungamenti disciplinati in altri articoli.

Hanno quindi diritto all'utilizzo degli strumenti e ai relativi accessi solo i soggetti autorizzati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno, nello specifico a:

1. l'utilizzo del computer o di altre apparecchiature;
2. l'utilizzo della posta elettronica;
3. l'accesso ad Internet.

Soggetti non autorizzati che accedono agli strumenti informatici di Ateneo sono perseguiti secondo norma

1.5 Titolarità di apparecchiature e dati (*)

L'Ateneo è esclusivo titolare e proprietario delle apparecchiature acquistate con fondi propri (centrali o dipartimentali) e messi a disposizione dei soggetti autorizzati ai soli fini dell'attività lavorativa.

L'Ateneo è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante le proprie apparecchiature digitali o archiviati in modo cartaceo nei propri locali.

Il soggetto autorizzato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nelle apparecchiature di Ateneo (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i file di filmati o altre tipologie di file) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'Ateneo.

Nel caso di strumenti di proprietà dell'Ateneo, il soggetto non può impedire l'installazione o la presenza di software (agenti, o comunque denominati) nei device di accesso, necessari alla sicurezza informatica propria e dell'Ateneo. L'installazione può essere differenziata per specificità di rapporto di lavoro, ed è regolata da periodiche circolari del Rettore o del Direttore Generale.

1.6 Finalità nell'utilizzo delle apparecchiature

Le apparecchiature assegnate sono uno strumento nelle disponibilità del soggetto autorizzato primariamente per un fine di carattere istituzionale e/o lavorativo: le finalità private e diverse da quelle di Ateneo devono essere ritenute residuali.

1.7 Trasferimento di dati con supporti digitali

Il trasferimento di dati sia all'interno che all'esterno dell'Ateneo tramite supporti digitali deve seguire le sottostanti avvertenze, atte a proteggere le informazioni trasferite da potenziali intercettazioni, copie, modifiche, errori di instradamento o distruzione.

- L'invio di comunicazioni può avvenire solo da apparecchiature protetti da antimalware, onde proteggere le comunicazioni da eventuali software malevoli.
- Gli allegati contenenti "dati particolari" (ex art. 9 GDPR) o "dati giudiziari" (ex art. 10 GDPR) oppure informazioni confidenziali, come sopra definite, devono essere oggetto di invio come allegato criptato con chiavi di cifratura allo stato dell'arte.
- In caso di trasferte fuori dall'ufficio, utilizzando le apparecchiature in contesto pubblico, è necessario prestare la massima attenzione che terzi non autorizzati non possano accedere ai dati.

2. Password

2.1 Le password

Le password sono un metodo di autenticazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

Il livello di protezione al processo di autenticazione (ad es. l'autenticazione a più fattori, l'uso di token HW/SW, il ricorso a chiavi di sicurezza, etc.) viene deciso dall'Amministrazione e periodicamente aggiornato in base allo standard delle possibili minacce e delle misure di prevenzione disponibili, secondo apposita procedura, gestita e monitorata dalla Direzione competente sui Servizi Informativi.

Al fine di proteggere l'Ateneo dall'obsolescenza dei sistemi di protezione, gli account che non vengono utilizzati per un periodo superiore ai sei mesi verranno disattivati dall'Ateneo.

In qualsiasi momento l'Ateneo si riserva il diritto di revocare al soggetto il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

2.2 Regole per la corretta gestione delle password

Il soggetto autorizzato, per una corretta e sicura gestione delle proprie password, è tenuto a rispettare le regole seguenti:

1. le password sono assolutamente personali e non vanno mai comunicate ad altri;
2. occorre cambiare immediatamente una password non appena si abbia il minimo dubbio che sia diventata poco sicura;
3. i criteri di creazione di una nuova password sono come indicato dall'Amministrazione in apposita procedura, costantemente aggiornata in ragione del livello delle minacce possibili;
4. le password non devono essere memorizzate in chiaro su alcun tipo di supporto, quali, ad esempio, post-it (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. va assolutamente evitato di digitare la propria password in presenza di altri soggetti, anche se collaboratori o dipendenti dell'Ateneo, in grado di prendere visione dell'inserimento dei caratteri.

L'Amministrazione può valutare di prevedere, nell'apposita procedura di gestione, meccanismi automatici che consentano un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per un periodo di tempo definito viene considerato un attacco al sistema e l'account viene bloccato per un periodo di tempo definito.

In caso di problemi deve essere immediatamente contattato il tecnico informatico di riferimento.

2.3 Modifica della password

Ogni soggetto autorizzato può variare la propria password di accesso in modo autonomo.

La password deve poter essere sostituita anche qualora l'utente l'abbia dimenticata.

2.4 Audit delle password

Nell'ambito delle attività riguardanti la tutela della sicurezza della infrastruttura tecnologica e informandone preventivamente tutti i soggetti interessati, l'Ateneo può effettuare analisi periodiche sulle password al fine di verificarne la solidità (ad esempio ricorrendo a data base deputati a segnalare password compromesse a livello internazionale) le policy di gestione e la durata.

Nel caso in cui l'audit abbia, tra gli esiti possibili, la decodifica o il riconoscimento della password, questa viene bloccata e all'interessato viene richiesto di cambiarla.

3. Operazioni a protezione della postazione di lavoro

In questa sezione vengono trattate le operazioni a carico del soggetto autorizzato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio d'Ateneo.

3.1 Login e Logout

Il "Login" è l'operazione con la quale l'autorizzato si connette al sistema informativo di Ateneo o ad una parte di esso, dichiarando il proprio Username e Password (Account), aprendo una sessione di lavoro.

In molti casi non è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), poiché di norma è previsto automaticamente il Single Sign On – SSO – per evitare che ogni applicativo i richieda un username e una password.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

3.2 Rete di Ateneo

La rete di Ateneo è uno strumento e paradigma informatico che consente di condividere risorse digitali. Il comportamento da seguire per l'uso oltre che dato dalle presenti Linee Guida deriva anche dall'Acceptable User Policy del GARR poiché l'Ateneo rappresenta un "nodo" nazionale gestito dallo stesso GARR. Esso è parte integrante delle presenti Linee Guida.

3.3 Dispositivi connessi alla rete di Ateneo

Di norma i dispositivi utilizzati per l'espletamento delle proprie mansioni lavorative, didattiche o per l'erogazione dei servizi richiesti dal rapporto con il quale si è legati all'Ateneo sono fornite e gestite dai centri di costo dell'ateneo e sono collegati alla rete universitaria (cablata o wireless), o alle sue estensioni (presso AOUI ed ESU).

Nel caso in cui l'attività lavorativa o di ricerca sia svolta in spazi e luoghi che non afferiscono direttamente

all'Ateneo l'utilizzatore può far uso del servizio VPN di Ateneo ed operare esattamente come se ci si trovasse all'interno della rete universitaria.

In entrambi i casi il dispositivo dal quale l'utente accede si trova all'interno di uno spazio di indirizzamento affidato in gestione esclusiva all'Università di Verona, che nella fattispecie è caratterizzato dalla classe IP contenuta nella rete 157.27.0.0/16, e dagli indirizzi delle classi private, utilizzati per erogare servizi mediante dispositivi che non devono essere raggiungibili dalla rete internet

Le comunicazioni da e verso internet che avvengono all'interno di tale perimetro, che comunica con internet attraverso la rete GARR, sono sottoposte alle normative vigenti relativamente alla conservazione dei dati di traffico delle comunicazioni.

3.4 Dispositivi di Ateneo

I dispositivi connessi alla rete di Ateneo/universitaria sono contraddistinti dal fatto che nel momento in cui si collegano alla rete internet si presentano con un indirizzamento (indirizzo IP) che ne deve consentire una identificazione univoca.

L'identificazione dei dispositivi connessi alla rete di Ateneo viene effettuata mediante un sistema che adotta lo standard internazionale IEEE 802.1x utilizzando protocolli e metodi sicuri, che eventualmente sono progressivamente adeguati in funzione dei requisiti di sicurezza che si palesano nel tempo.
Le credenziali di autenticazione alla rete sono collegate al sistema di Gestione delle Identità di Ateneo (GIA) mediante il quale è in tal modo possibile associare al dispositivo la persona che ne fa uso.
I dispositivi devono essere altresì catalogati all'interno del servizio di Directory Service fornito dalla Direzione Sistemi Informativi.

3.5 Dispositivi Personali e BYOD

Il soggetto, per qualunque ragione, può far uso di dispositivi personali, non riconducibili ad alcuna struttura di Ateneo, per attività compatibile con il proprio status e operatività: ad esempio il cellulare per navigare in internet.

Un caso particolare riferibile a tale contesto contesto prende il nome di Bring Your Own Device (BYOD), che significa che il soggetto effettua parte o tutta la propria prestazione lavorativa utilizzando il proprio device.

Al fine di utilizzare il proprio dispositivo, è responsabilità del soggetto garantire la sicurezza cibernetica propria e dell'Ateneo. Il dispositivo proprio non fa parte dell'inventario dell'Ateneo e pertanto non potrà ricevere supporto da parte dello stesso Ateneo.

3.6 Device generici

Si tratta di dispositivi funzionali che concorrono all'erogazione di servizi o svolgono funzioni specifiche, determinate e determinabili a priori (dispositivi multifunzione, citofoni, telefoni, dispositivi audio video, dispositivi di accesso, videocamere di sorveglianza, rilevatori di presenze, varchi di accesso, ecc), e che non dispongono della possibilità di configurazione in modalità avanzate, in considerazione delle loro funzioni della possibilità di configurazione in modalità avanzate, in considerazione delle loro funzioni limitate e circoscritte, sono collegati alla rete di ateneo utilizzando una rete interna con un indirizzamento che limita l'esposizione del dispositivo all'esterno o lo impedisce del tutto.

In considerazione di quanto sopra esposto, al fine di tutelare il transito nella rete delle informazioni che trasmettono nell'ambito delle funzioni che svolgono, nella definizione dell'architettura del servizio dovrà essere prestata estrema attenzione all'introduzione di accorgimenti alternativi che preservino i dati trasmessi (cifratura dei dati con protocolli sicuri, limitazione dei dispositivi che possono colloquiare, enforcement delle credenziali di autenticazione, ecc..).

Per tali dispositivi, dovrà essere redatto apposito inventario dei dispositivi comprensivo delle caratteristiche fisiche e funzionali di ogni dispositivo (ad es. Marca, modello, numero di serie, indirizzo fisico della scheda di

rete, ecc..) nonché dei riferimenti del responsabile amministrativo e del referente tecnico, al fine di poter disporre di un contatto nel momento in cui, a seguito di verifiche effettuate mediante sistemi di scansione delle vulnerabilità, si ravvisino condizioni che possano mettere a repentaglio la sicurezza di tutti i dispositivi connessi alla rete.

3.7 Server (*)

Strumenti collegati alla rete di Ateneo che erogano servizi sono definiti con il nome di Server. Tali dispositivi devono essere gestiti secondo norma, ad esempio prevedendo Amministratori di Sistema, garantendo l'applicazione di standard di sicurezza, e quanto altro previsto per sistemi server.

4. Uso di computer universitario

I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato.

L'Ateneo non effettua il backup dei dati memorizzati localmente nei device e non garantisce, quindi la sicurezza dei dati in essi presenti.

Ciò non impedisce di provvedere in autonomia: se si provvede in autonomia ad un backup della propria macchina (es. su disco esterno), questo deve essere sottoposto a crittografia.

I tecnici informatici possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno pericolosi per la sicurezza, sia sui sistemi degli utenti che sulle unità di rete e, qualora ciò non risulti possibile, disconnettere il device dalla rete e/o sospendere l'account dell'utente.

4.1 Corretto utilizzo del computer universitario (*)

Il computer consegnato al soggetto autorizzato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare problematiche di sicurezza, disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password, che deve essere custodita dall'autorizzato con la massima diligenza e non divulgata.

Per necessità di Ateneo, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere sia alla memoria di massa locali di rete (repository e backup) che ai server di Ateneo nonché, previa comunicazione al dipendente, accedere al computer, anche da remoto.

In particolare, l'utilizzatore del computer deve adottare le seguenti misure:

1. utilizzare solo ed esclusivamente le aree di memoria della rete o del cloud autorizzato dell'Ateneo ed ivi creare e registrare file e software o archivi dati;
2. spegnere il computer, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché 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;
3. mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'Ateneo;
4. non dare accesso al proprio computer ad altri utenti, a meno che siano soggetti con cui condividono l'utilizzo dello stesso computer o a meno di necessità stringenti e sotto il proprio costante controllo.

4.2 Divieti nell'utilizzo del computer universitario (*)

All'utilizzatore del computer è vietato:

1. gestire e memorizzare (anche temporaneamente) file, documenti e/o informazioni personali proprie o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa di Ateneo e negli strumenti informatici di Ateneo in genere;
2. modificare le configurazioni già impostate sul personal computer;
3. utilizzare programmi e/o sistemi di criptazione dei dati che non permettano poi all'Ateneo di accedervi per diversi scopi, anche di natura giudiziaria;
4. installare software di cui l'Ateneo non possieda la licenza;
5. caricare sul disco fisso del computer o nel server file diversi da quelli necessari allo svolgimento delle mansioni affidate.
6. implementare servizi di ambito di rete o sistemistici senza preventiva autorizzazione;
7. collegare di propria iniziativa apparati attivi di rete, come ad esempio access point wireless, switch, router, firewall, etc.., indipendentemente dal livello di sicurezza che questi sono in grado di offrire;

All'utilizzatore del computer è inoltre fatto severamente divieto di:

1. memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
2. creare e diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Ateneo, quali per esempio virus, trojan horses, etc.
3. accedere ad informazioni riservate o comunque non necessarie per le mansioni svolte;
4. utilizzare la rete per l'invio non autorizzato di materiale pubblicitario e/o promozionale o per comunicazioni massive dirette a gruppi di soggetti, siano essi afferenti o meno all'Ateneo;
5. riprodurre o duplicare programmi informatici tutelati dalla normativa sul diritto d'autore.

5. Antivirus

I virus informatici possono essere trasmessi tramite scambio di file via internet, mail, supporti removibili, chat, etc.

L'Ateneo impone su tutte le postazioni di lavoro / studio l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

Il soggetto autorizzato è tenuto a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti:

1. comunicare all'Ateneo ogni anomalia o malfunzionamento del sistema antivirus;
2. comunicare all'Ateneo eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, al soggetto autorizzato è vietato:

1. accedere alla rete di Ateneo in assenza di servizio antivirus attivo e aggiornato;
2. ostacolare l'azione dell'antivirus di Ateneo;
3. disattivare l'antivirus, soprattutto nel caso di installazione di software sul computer.

5. Accesso alla rete e ai servizi d'Ateneo

5.1 Soggetti con diritto di accesso alla rete ed ai servizi di Ateneo

Sono da considerarsi autorizzati all'accesso alla rete dati di Ateneo: dipendenti e studenti dell'Ateneo e tutti coloro che hanno un rapporto di lavoro, di collaborazione, di ricerca o di didattica, anche a tempo determinato, o che sono interessati alla fruizione di contenuti bibliotecari, purché riconosciuti nominalmente da un atto formale dell'Ateneo.

Nella categoria di atto formale d'Ateneo sono ricomprese le attestazioni puntuali di docenti, ricercatori e dirigenti: in quest'ultimi caso, unicamente per rapporti di durata definita e circoscritta (ad es. *visiting professor*).

Ai soggetti autorizzati sono fornite opportune credenziali di accesso e autenticazione, previa acquisizione dei dati dell'utente, come da procedure adottate e secondo quanto previsto dalle norme vigenti.

Il personale docente, ricercatore e tecnico-amministrativo strutturato, all'interruzione del rapporto di lavoro, viene concesso di poter utilizzare alcuni servizi (casella di posta elettronica, accesso ad Internet, servizi ad essa correlati come la VPN e l'accesso a riviste e banche dati elettroniche, fatti salvi i limiti contrattuali previsti da alcuni editori) per un tempo indefinito, salvo richiesta del diretto interessato di disattivare prima l'utenza.

Per quanto concerne gli studenti e le studentesse, al termine o all'interruzione del percorso degli studi e al fine di permettere continuità con le numerose proposte di formazione nonché iniziative generali per la categoria degli "Alumni" erogate dall'Ateneo, è previsto un periodo di Grazia di 5 anni con esclusione per chi ha optato in senso negativo al trattamento nella banca dati Alma Laurea. In questo periodo viene concesso di poter utilizzare alcuni servizi (casella di posta elettronica, accesso ad Internet, servizi ad essa correlati come la VPN e l'accesso a riviste e banche dati elettroniche, fatti salvi i limiti contrattuali previsti da alcuni editori)

All'interruzione del rapporto con personale non strutturato docente, ricercatore e tecnico amministrativo, viene concesso di poter utilizzare alcuni servizi (casella di posta elettronica, accesso ad Internet, servizi ad essa correlati come la VPN e l'accesso a riviste e banche dati elettroniche, fatti salvi i limiti contrattuali previsti da alcuni editori) per un tempo massimo di 5 anni, salvo richiesta del diretto interessato di disattivare prima l'utenza.

Qualora il corpo studentesco o il personale non strutturato necessitino di un'ulteriore proroga nel mantenimento dei servizi di cui sopra, possono avanzare richiesta motivata al Rettore, previamente sottoscritta dal Direttore di Dipartimento.

In ogni caso, per tutti i soggetti, periodicamente verrà effettuata apposta comunicazione in relazione ai diritti di inerenti al trattamento dei dati personali. Nel periodo di Grazia, in caso di inutilizzo per dodici mesi, le credenziali vengono disattivate previa comunicazione via email.

5.2 Accreditamento utenti

Il processo di accreditamento viene avviato quando una struttura dell'Ateneo richiede di consentire l'accesso o modificare le autorizzazioni di accesso alle risorse informatiche universitarie da parte di soggetti autorizzati.

Il processo è svolto dal responsabile della struttura di afferenza del soggetto autorizzato o da personale da questi delegato come da vigente procedura di Ateneo.

Il responsabile del processo provvede all'identificazione del soggetto autorizzato e all'accertamento dei requisiti necessari per l'accreditamento e, di fronte ad esito positivo, crea o aggiorna il profilo anagrafico in accordo.

L'Amministrazione, quindi, provvede all'accreditamento informatico attraverso il sistema di Identity Management in adozione, che permette la gestione automatica del ciclo di vita (creazione, modifica, disabilitazione) delle identità e delle credenziali elettroniche degli utenti.

Il processo di accreditamento degli utenti si basa sulla integrazione tra risorse autorevoli e risorse popolate (destinatarie di sincronizzazione delle credenziali) e su deleghe amministrative garantite dal sistema di Identity Management.

Gli utenti sono classificati sulla base dell'appartenenza a classi e sottoclassi di Identità.

I ruoli nella gestione delle identità e le responsabilità ai sensi del GDPR sono definiti sulla base della posizione organizzativa e delle attribuzioni formali conseguenti, sia di carattere collettivo che individuale.

Le classi di identità relativi ai ruoli utenti sono organizzate nel processo di accreditamento come da vigente procedura, cui si rinvia per i dettagli operativi.

A titolo esemplificativo, le classi sono le seguenti:

- Studenti [Iscritti, Specializzandi, Post-Lauream, Laureati]: per questa classe le risorse autorevoli sono applicativi e data base ufficiali di gestione anagrafica e carriere degli studenti;
- Personale [Docenti e Ricercatori, Dottorandi, Tecnico-Amministrativi]: per questa classe le risorse autorevoli sono applicativi e gestionale di backoffice e di gestione della carriera giuridico-economica del personale.
- Esterni [Consulenti, Fornitori, Ospedalieri, Collaboratori 150H]: per questa classe le risorse autorevoli sono applicativi e gestionale di backoffice e di gestione giuridico-economica del personale esterno.
- Frequentatori [Ospiti, Congressisti, Studenti ospiti, Studenti frequentatori, Frequentatori biblioteca]: per questa classe la risorsa autorevole è lo stesso sistema di Identity Management attraverso funzionalità delegate a responsabili e referenti di ciascuna struttura d'Ateneo.

6. Internet

La connessione alla rete internet dall'apparecchiatura in dotazione è prevista per motivi attinenti allo svolgimento dell'attività istituzionale e/o lavorativa.

L'utilizzo per scopi personali è permesso con moderazione e seguendo gli accorgimenti previsti dal presente Disciplinare.

6.1 Misure preventive per ridurre navigazioni illecite (*)

L'Amministrazione può adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa, di cui viene dato conto nelle corrispondenti procedure, mantenute costantemente aggiornate dalle strutture competenti.

6.2 Divieti concernenti la navigazione internet (*)

A meno che non possa essere giustificato per motivi legati al rapporto di lavoro in essere, non è consentito:

1. accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap;
2. scaricare software (anche gratuito) da siti internet;
3. effettuare transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisti on-line e simili;
4. effettuare qualsiasi registrazione a siti internet i cui contenuti non siano riconducibili all'attività lavorativa;
5. partecipare a forum non professionali, o utilizzare chat line e bacheche elettroniche, o partecipare a gruppi di discussione, o lasciare commenti ad articoli, o iscriversi a mailing list, spendendo il logo o la denominazione dell'Università, salvo specifica autorizzazione del Rettore o del rispettivo Direttore di Dipartimento o Dirigente;
6. archiviare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
7. promuovere utile o guadagno personale attraverso l'uso di internet o della posta elettronica di Ateneo;
8. accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure adottate dall'Università.
9. creare siti web personali sui sistemi dell'Università, salvo specifica autorizzazione del Rettore o del rispettivo Direttore di Dipartimento o Dirigente.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di internet, nonché un possibile illecito trattamento di dati personali, è ricondotta nella responsabilità personale del soggetto inadempiente.

6.3 Sabotaggio (*)

È vietato accedere a siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'ente per bloccare accessi non conformi all'attività lavorativa.

In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tali fini.

6.4 Diritto d'autore

È vietato utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) secondo le procedure vigenti.

7. Posta elettronica

7.1 La posta elettronica come strumento di lavoro e studio

Tutti gli indirizzi di posta elettronica appartenenti al dominio univr.it (o a domini di terzo livello o superiori livelli di univr.it) sono espressione dell'Università di Verona e della sua struttura organizzativa, pertanto il loro utilizzo è connesso all'attività istituzionale e lavorativa.

L'Ateneo è consapevole della possibilità di un limitato utilizzo personale della posta elettronica, comunque soggetto alle disposizioni del presente Disciplinare.

Nell'interesse primario di tutti i titolari di casella di posta elettronica dell'Ateneo, in caso di ricezione sulla casella di e-mail di natura personale, si raccomanda di cancellare ogni messaggio al fine di evitare ogni eventuale e possibile back up dei dati: tutti i contenuti non cancellati possono essere soggetti a back up.

Quale misura volta a prevenire possibili utilizzi illeciti dalla casella e-mail universitaria, tutti i titolari sono tenuti ad allertare in via cautelativa i tecnici informatici di riferimento ogniqualvolta a messaggi ricevuti siano allegati file eseguibili e/o di natura incomprensibile o non conosciuta.

Nel caso di mittenti sconosciuti o messaggi inusuali, od anche di messaggi provenienti da mittenti noti ma che contengono allegati sospetti, per non correre il rischio che l'apparecchiatura possa essere infettata da virus informatici, si raccomanda di cancellare i messaggi senza aprirli oppure allertare in via cautelativa i tecnici informatici di riferimento.

Si raccomanda, riassuntivamente, di mantenersi aggiornati sulle periodiche informative in materia di sicurezza nell'uso della posta elettronica condivise nell'Intranet universitaria dalla Direzione competente sui Servizi Informativi.

Come da vigente procedura gestita dalla Direzione competente sui Servizi Informativi, a richiesta dei responsabili di struttura o di personale da questi delegato, è prevista l'attivazione di caselle istituzionali di posta elettronica condivise tra più dipendenti.

Per tali caselle sono adottate regole di composizione degli indirizzi di posta elettronica, omogenee per tutto l'Ateneo, tali da identificare immediatamente le strutture organizzative o i servizi cui fanno riferimento.

Si raccomanda l'utilizzo prioritario delle caselle istituzionali a tutti i dipendenti che operano nell'ambito di gruppi di lavoro e/o uffici, in modo da consentire l'accesso ai messaggi urgenti ad almeno uno dei componenti del team.

Anche per l'accesso alle caselle di posta elettronica, il livello di protezione al processo di autenticazione, (ad es. l'autenticazione a più fattori, l'uso di token HW/SW, il ricorso a chiavi di sicurezza, etc.) viene deciso dall'Amministrazione e periodicamente aggiornato in base allo standard delle possibili minacce e delle misure di prevenzione disponibili, secondo apposita procedura, gestita e monitorata dalla Direzione competente sui Servizi Informativi.

7.2 Divieti concernenti l'utilizzo della posta elettronica

È vietato:

1. creare, archiviare o spedire, anche solo all'interno della rete d'Ateneo, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività istituzionale o lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto o in genere a pubblici dibattiti utilizzando l'indirizzo di posta universitario;
2. sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non connesse al ruolo istituzionale o lavorativo;

3. inviare, tramite la posta elettronica, anche all'interno della rete d'Ateneo, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico;
4. inviare messaggi di posta elettronica, anche all'interno della rete d'Ateneo, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

7.3 Posta elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata si raccomanda l'attivazione del servizio di risposta automatica previsto dall'applicativo di gestione della posta elettronica universitaria.

7.4 Cessazione del rapporto

Alla cessazione del rapporto di lavoro, per il personale docente, ricercatore e tecnico amministrativo, e al conseguimento del titolo di studio e/o interruzione, per gli studenti, i termini e le modalità di conservazione e disabilitazione della casella di posta elettronica nominativa sono quelli indicati al paragrafo 5.1 per la generalità dei servizi degli utenti d'Ateneo.

7.5 Memorizzazione dei file di Log

I sistemi che memorizzano i file di Log sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione come, ad esempio, la cosiddetta "rotazione dei log file") i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia imposta da vigenti norme, regolamenti o policy.

Per quanto riguarda il trattamento dei dati di Log:

- i dati di Log raccolti, dopo un periodo di trenta giorni, sono conservati in forma crittografata. Le chiavi di crittografazione e decrittografazione sono mantenute dal Titolare e dal Dirigente della Direzione competente;
- la conservazione di dati di Log, sia crittografati che non, avviene per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive, di sicurezza e di controllo e per quanto dispone la normativa in materia;
- il trattamento dei dati di log avviene in due modalità diverse:
  - per quanto concerne i dati di log raccolti e non ancora memorizzati in modalità crittografata, il trattamento viene effettuato dal Dirigente della Direzione competente, dal personale dell'Area che sovraintende le reti e dell'Area che sovraintende i sistemi della Direzione competente che, in forza del presente Regolamento, sono da considerarsi incaricati a trattare i dati di log nelle modalità strettamente necessarie nell'ambito dell'espletamento delle azioni ordinarie e quotidiane di mantenimento della rete e delle risorse, oltre che nell'ambito del trattamento previsto dal loro status individuale di amministratore di sistema;
  - ogni trattamento riferibile a dati di log già memorizzati in forma crittografata deve avvenire solamente a seguito di istanza presentata dagli organi competenti di pubblica sicurezza o dal Titolare.

8. Uso di altre apparecchiature

8.1 Device mobili (notebook, tablet o smartphone)

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in “device mobili”) possono venire concessi in uso dall'Ateneo ai soggetti autorizzati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'Ateneo.

L’utilizzatore è responsabile dei device mobili assegnatigli dall'Ateneo e deve custodirli con diligenza sia durante gli spostamenti sia durante l’utilizzo nel luogo di lavoro.

In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti e la segnalazione all’ufficio competente in materia di trattamento e protezione dei dati personali, secondo le vigenti procedure.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Ateneo per il tramite della Direzione competente sui Servizi Informativi.

I device mobili che permettono l’attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti incustoditi privi di PIN.

8.2 Memorie esterne

Ai soggetti autorizzati può essere assegnata una memoria esterna (ad es. chiave USB, hard disk esterno, memory card) su cui copiare temporaneamente dei dati per un facile trasporto.

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all’articolo precedente e, soprattutto, devono essere utilizzati esclusivamente dai soggetti cui sono state affidate e in nessun caso essere consegnate a terzi.

8.3 Device personali

I dispositivi personali possono essere utilizzati dal personale e collaboratori dell’Ateneo per l’attività istituzionale e lavorativa, purché sul dispositivo personale siano soddisfatte le misure di sicurezza minime previste dalle procedure vigenti, costantemente aggiornate dalla Direzione competente sui Servizi Informativi e rese note e accessibili agli utilizzatori in apposita pagina intranet.

A titolo esemplificativo gli utilizzatori sono tenuti a verificare che su tali apparecchiature:

1. siano installate le ultime versioni di sistemi operativi e di software applicativi supportati dai produttori;
2. siano installate automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni;
3. siano installati strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali) e che tali strumenti siano mantenuti aggiornati in modo automatico;
4. venga eseguita automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.

Si raccomanda che eventuali dati, utilizzati per finalità istituzionale / lavorativa e particolarmente importanti per l’Ateneo o che rivestano il carattere della personalità o della riservatezza, vengano alternativamente o salvati sulle aree di condivisione protetta di Ateneo o salvati localmente solo con cifratura.

8.4 Utilizzo delle stampanti

L'Ateneo mette a disposizione di dipendenti e collaboratori unità periferiche di stampa ad uso esclusivamente istituzionale e lavorativo.

I dipendenti e collaboratori sono tenuti ad effettuare la stampa dei dati solo se necessaria all'attività lavorativa e a ritirarla prontamente dai vassoi delle stampanti comuni, in modo da evitare che sia visibile o possa essere raccolta da terzi.

L'Ateneo è dotato di un sistema con stampa previa autenticazione con badge, permettendo così di ritirare la stampa presso qualsiasi stampante di Ateneo.

8.5 Restituzione, riutilizzo e distruzione dei device

Ogni device ed ogni memoria esterna affidati ai soggetti autorizzati (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, etc.), al termine del loro utilizzo (per qualsiasi causa) dovranno essere restituiti all'Ateneo che provvederà a ricondizionarli seguendo le norme di legge in vigore al momento e procedure certificate a livello internazionale, al fine di loro riutilizzo interno o della loro cessione a terzi come da vigenti procedure di riuso solidaristico, o eventualmente a distruggerli in modo sicuro.

In particolare, l'Ateneo provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati, tramite:

- Distruzione fisica del supporto
- Cancellazione Logica (Wiping)
- Smagnetizzazione (Degauss)

9. Cloud (*)

9.1 Cloud Computing

Con il termine *cloud computing* si indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on-demand attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Le risorse non vengono pienamente configurate e messe in opera dal fornitore per l'utente, ma vengono a questi assegnate, rapidamente e convenientemente, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti, lasciando all'utente parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'Ateneo a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farm di aziende che spesso risiedono in uno stato extraeuropeo, configurando un trasferimento dei dati all'estero. Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti,

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili. Si vincola tale utilizzo alla presenza della VPN.

L'uso di In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'Ateneo, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

9.2 Utilizzo di sistemi cloud

È vietato l'utilizzo di sistemi Cloud non espressamente approvati dall'Ateneo, per il tramite della Direzione competente sui Servizi Informativi, nel rispettivo di specifiche procedure di controllo che verifichino i requisiti di sicurezza informatica e di protezione dei dati personali.

A titolo esemplificativo, per essere approvati i sistemi cloud devono:

1. essere sistemi cloud di cui si conosce l'esatto posizionamento dei server e per i quali si è predisposto quanto richiesto dalle norme, compreso eventualmente quello che è richiesto per il trasferimento dei dati all'estero;
2. forniti da ditte / soggetti preventivamente nominati Responsabile al Trattamento dei dati da parte dell'Ateneo, soggetti a tutti i controlli previsti dalla normativa (ex art. 28 GDPR).

10. Gestione dei dati su supporto cartaceo (*)

10.1 Archivi amministrativi cartacei

Per quanto riguarda in generale la documentazione cartacea, i soggetti autorizzati sono tenuti a:

1. gestire con cura gli atti e i documenti amministrativi contenenti dati personali o comunque riservati per tutta la durata delle attività istituzionali o lavorative presidiate e successivamente riporli in archivi ad accesso controllato al fine di escluderne l'accesso, da parte di persone non autorizzate al trattamento (stanze, armadi, cassetti chiusi a chiave). A questo proposito sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto;
2. utilizzare, se disponibili, gli appositi apparecchi "distruggi documenti" qualora si renda necessario distruggere i documenti contenenti dati personali, oppure rendere comunque inaccessibili i dati in essi contenuti prima dello smaltimento;
3. adottare opportune cautele per salvaguardare la riservatezza dei dati personali nei flussi di documenti cartacei all'interno degli uffici (ad es. trasmettere documenti in busta chiusa);
4. ove possibile, evitare la stampa di documenti digitali;
5. ove possibile, effettuare la scansione dei documenti cartacei ed archiviarli digitalmente;
6. rimuovere immediatamente ogni documento cartaceo da spazi comuni, per evitare che siano prelevati o visionati da terzi non autorizzati.

10.2 Archivi di pubblico interesse, per scopi di ricerca storica o statistica

Nell'ambito dei trattamenti di dati personali effettuati per scopi di ricerca storica, statistica o sanitaria e la conservazione di documenti presso gli archivi dell'Ateneo, i soggetti autorizzati, debitamente istruiti, sono tenuti al rispetto delle vigenti disposizioni normative e **r**egole deontologiche.

I Dipartimenti, i Centri e le Biblioteche dell'Ateneo predispongono e garantiscono l'accesso alle risorse documentali cartacee ed elettroniche per le esigenze dell'utenza, come descritto nelle rispettive Carte di servizi, ove presenti, e attenendosi alle procedure e alle regole interne (ad es. procedure di sicurezza degli archivi, etc.).

10.3 Clear Desk Policy

I soggetti autorizzati al trattamento sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle attività ad essi demandate, di tutti gli atti e documenti contenenti dati personali e non.

Conseguentemente l'Ateneo raccomanda di adottare una Clear Desk Policy (Politica della scrivania pulita): trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'Ateneo.

I principali benefici di una politica della scrivania pulita sono:

- Minor rischio che informazioni confidenziali possano essere viste da persone non autorizzate;
- Minor rischio che documenti confidenziali possano essere sottratti o smarriti.

In particolare, si raccomanda di non lasciare in vista sulla propria scrivania documenti cartacei quando ci si allontana oppure quando è previsto un incontro con un soggetto non autorizzato alla conoscenza dei dati in essi contenuti; quindi a riporre in luogo sicuro (armadio, cassettiera, archivio, etc.) tutti i documenti cartacei, affinché gli stessi non possano essere visti da terzi non autorizzati (ad es. addetti alle pulizie, personale di prima accoglienza, etc.).

11. Controllo

L'Ateneo, in qualità di titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo, anche preventivo;
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico.

Per tali controlli l'Ateneo si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'Ateneo non adotta apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (ex L. n. 300/1970, art. 4, comma 1) anche qualora tali funzioni fossero consentite dalle apparecchiature e dai software utilizzati dall'Ateneo

11.1 Modalità di verifica

Conformemente al GDPR, alla normativa nazionale in materia di trattamento dei dati e ai provvedimenti delle competenti Autorità di controllo, l'Ateneo promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili a tutti soggetti autorizzati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Ateneo informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte di dipendenti e collaboratori avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Possono essere svolte verifiche programmate in ordine a dimostrare la conformità delle attività di trattamento alle disposizioni normativa e l'efficacia delle misure di sicurezza adottate, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

È comunque in costante revisione un "inventario dei trattamenti dati" ai fini di logging e sicurezza.

Tale inventario è reso disponibile agli utenti.

11.2 Modalità di Conservazione

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione a:

1. esigenze tecniche o di sicurezza;
2. indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
3. obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate.

12. Amministratori di sistema

Ai fini della corretta gestione di tutti i dati e le informazioni che transitano sulle reti e nelle banche dati dell'Ateneo, per ciascun sistema informatizzato vengono individuati soggetti particolarmente esperti, chiamati a svolgere funzioni di gestione e vigilanza sul corretto utilizzo di tali asset istituzionali.

L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, che deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La designazione quale amministratore di sistema è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni loro attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante per la Protezione dei Dati Personali.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing l'Ateneo, quale titolare del trattamento, è tenuto a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di verifica da parte dell'Ateneo, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Per l'espletamento delle richiamate attività l'Ateneo segue la vigente procedura, demandata al Responsabile dei Servizi Informativi.

13. Provvedimenti disciplinari

Il presente Disciplinare si integra con normativa e strumenti regolatori delle condotte di personale e studenti, in particolare:

a. il Codice di Comportamento dei Dipendenti Pubblici (DPR n. 62/2013), che costituisce la base minima per i codici di comportamento di tutte le pubbliche amministrazioni;
b. il Codice di Comportamento del Personale dell'Università di Verona;
c. il Codice Etico dell'Università, che si applica a tutta la comunità universitaria - dipendenti e studenti - determinando i valori fondamentali dell'Ateneo, promuovendo il riconoscimento e il rispetto dei diritti individuali, nonché l'accettazione di doveri e responsabilità nei confronti dell'istituzione, dettando altresì le regole di condotta nell'ambito della comunità.

La violazione dei doveri contenuti in tali Codici è fonte di responsabilità disciplinare ai sensi della normativa e dei regolamenti d'Ateneo nel tempo vigenti.

La violazione dei doveri rileva, altresì, ai fini della responsabilità civile, amministrativa e contabile, qualora le stesse responsabilità siano collegate alla violazione di doveri, obblighi, leggi e regolamenti.

L'istruttoria dei procedimenti disciplinari nei confronti del personale docente e ricercatore è svolta dal Collegio di disciplina, che esprime parere sui provvedimenti da adottare; conseguentemente il Consiglio di Amministrazione, in conformità al parere, irroga la sanzione o dispone l'archiviazione.

L'istruttoria dei procedimenti disciplinari nei confronti del personale dirigente e tecnico-amministrativo è svolta dall'Ufficio di disciplina: al termine del procedimento il Direttore Generale o l'Ufficio di disciplina, a seconda della gravità del comportamento contestato, irroga la sanzione.