REGOLAMENTO INTERNO

Regole di condotta ed obblighi dei responsabili ed incaricati del trattamento dei dati personali, in relazione all'uso degli strumenti informatici, di Internet e della Posta Elettronica, redatto ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata in GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei ed adeguato al Regolamento Europeo 679/2016.

Il presente documento è proprietà dell'Università degli Studi Link Campus University
Sono vietate copie e distribuzioni non espressamente autorizzate

REV.	DATA	CAUSALE	REDAZIONE	VERIFICA	APPROVAZIONE
1.0	15/02/2024	Prima redazione	V. Iellamo	R. Russo	R. Russo

1. SEZIONE I - Ambito generale

1.1. Definizioni

Università degli Studi Link. Via del Casale di San Pio V, 44 - 00165 Roma P. IVA 11933781004 (di seguito **Università**)

Autorizzazione: il provvedimento adottato dal Garante con cui il titolare del trattamento (ente pubblico, impresa, libero professionista) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, ovvero a trasferire dati personali all'estero.

Comunicazione: far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il responsabile o l'incaricato), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione (vedi anche diffusione)

Consenso: la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare).

D.Lgs. 196/2003: Decreto Legislativo 196 del 30 giugno 2003 e sue successive modifiche ed integrazioni.

Dato personale: qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo. Sono, ad esempio, dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; ma anche un'immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc.

Dato sensibile: un dato personale che, per la sua natura, richiede particolari cautele: sono dati sensibili quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Dato giudiziario: i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

Diffusione divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).

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

GDPR General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - UE 2016/679: è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE). Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018.

Incaricato: ogni dipendente o collaboratore, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'Università. Il regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4). In sede europea, alla nostra DPA è stato concesso di poter utilizzare ancora i termini titolare, responsabile e incaricato; traducendo così, nella versione italiana del GDPR, la figura del "*controller*" (Art. 4.7) con "*titolare del trattamento*"; "*processor*" (Art. 4.8) con "*responsabile del trattamento*"; "*third party*" (Art. 4.10) con "*terzo*", e di poter continuare ad utilizzare il termine "*incaricato*" per qualificare "*le persone autorizzate al*

trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Alla luce di ciò, si può identificare la figura di Incaricato in quella di Responsabile.
Informativa: le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il titolare e l'eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).
Interessato: la persona fisica cui si riferiscono i dati personali.
Misure di sicurezza: sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.
NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.
Responsabile (del trattamento): la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.
Titolare del trattamento: la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza).
Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.).
Trattamento (di dati personali): un'operazione o un complesso di operazioni che hanno per oggetto dati personali.

1.2. Premessa

L'ambito lavorativo porta la nostra Università a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono richiesti.
Tali informazioni possono essere considerate, ai sensi del D. Lgs. 196/2003 e successive modifiche ed integrazioni, "*dati personali*" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l'Università adotti una serie di misure minime ed idonee previste dalle norme.
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'Università è chiamata a garantire la riservatezza, o per accordo di non divulgazione, o per una più ampia tutela del patrimonio dell'Università.
Ai fini di questo regolamento si specifica, pertanto, che con il termine "*dati*" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore 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'Università 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 l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con

l'Università stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita.
Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.
La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, l'accesso alla rete internet dal computer, espone l'Università a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine della 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'Università ha adottato il presente Regolamento, diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature dell'Università.
Il presente Regolamento si applica ai responsabili e incaricati che si trovino ad operare con le risorse messe a disposizione dall'Università, oggetto di tutela da parte del presente documento, che sono:

- il patrimonio informativo, detenuto dall'Università, in formato elettronico;
- i servizi informatici erogati dall'Università;
- le postazioni di lavoro "fisse" (PC desktop e simili) e "mobili" (PC portatili e simili);
- i dispositivi cellulari (smartphone);
- i software di comunicazione;
- i server, le apparecchiature e tutto il materiale hardware in generale. dati dell'Università.

Una gestione dei dati cartacei, un uso dei computer e di altre attrezzature elettroniche (di seguito dispositivi), nonché dei servizi internet e della posta elettronica difforme dalle regole contenute nel presente Regolamento potrebbe esporre l'Università ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico dell'Università, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

1.3. Riferimenti normativi

Questo documento fa riferimento al seguente quadro normativo:

- "Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", che sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018 (d'ora in poi "GDPR");
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"(d'ora in poi "Codice");
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008).
- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".

1.4 Ambito di applicazione del presente documento

Il presente documento si applica ai soggetti di seguito indicati e, per brevità, definiti "*utenti*":

a) dirigenti e dipendenti, a qualsiasi titolo inseriti nell'organizzazione dell'Università, senza distinzione di ruolo e/o livello;
b) consulenti e collaboratori dell'Università, a prescindere dal rapporto contrattuale intrattenuto con la stessa;

c) dipendenti e collaboratori di società che hanno un contratto in essere con l'Università e che utilizzano le risorse messe a disposizione dalla stessa;
d) ospiti dell'Università, per l'eventuale uso delle risorse messe a disposizione dalla stessa;
e) enti e agenzie attestati alla rete Intranet, per quanto applicabile.

Le norme si rivolgono a differenti categorie di soggetti essendo destinate a disciplinare sia il comportamento di utenti "*meri utilizzatori*" (fruitori di PC desktop, smartphone, PC portatili, ecc.), sia il comportamento di utenti che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, ecc.).
Ciascun utente, in base al proprio profilo "*base*" o "*evoluto*", dovrà attuare le norme che sono allo stesso indirizzate e, nel caso di dubbi di applicazione delle stesse, potrà rivolgersi ai Sistemi Informativi di Ateneo.

1.5. Titolarità dei dispositivi e dei dati

L'Università è l'esclusiva titolare e proprietaria dei dispositivi messi a disposizione degli incaricati o dei responsabili, ai soli fini dell'attività lavorativa.
L'Università è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.
Il responsabile o l'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati memorizzati nei dispositivi dell'Università (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) 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'Università.

1.6. Finalità nell'utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità del responsabile o dell'incaricato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle istituzionali, se non eccezionalmente e nei limiti evidenziati dal presente Regolamento.
Qualsiasi eventuale tolleranza da parte di questa Università, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Regolamento.

1.7. Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo dell'incaricato o di consulenza del responsabile con l'Università o, comunque, al venir meno, ad insindacabile giudizio della stessa, della permanenza dei presupposti per l'utilizzo dei dispositivi dell'Università, i responsabili hanno i seguenti obblighi:
1. procedere immediatamente alla restituzione dei dispositivi in uso.
2. divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo.

1.8. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo dell'incaricato o di consulenza del responsabile con l'Università o, comunque, al venir meno, ad insindacabile giudizio della stessa, della permanenza dei presupposti per l'utilizzo di dati cartacei dell'Università, gli incaricati hanno i seguenti obblighi:
1. procedere immediatamente alla restituzione dei dati cartacei in loro possesso.
2. divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili, tramite qualsiasi processo.

1.9. Gestione degli incidenti e databreach

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato dall'utente in modo tempestivo ai Sistemi Informativi, che raccoglieranno le segnalazioni e avvieranno il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.
Nel caso in cui l'incidente sia di una certa gravità e riguardi il patrimonio informativo e di conoscenza detenuto dall'Università oppure le applicazioni informatiche, l'utente dovrà avvisare anche il responsabile della propria area di riferimento/appartenenza, oltre che i Sistemi Informativi.
Per gli incidenti che possono determinare una violazione dei dati personali, cioè la 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 (cd. "*databreach*"), l'art. 33 del GDPR prevede che "*il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*.".
Il successivo art. 34 disciplina il caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche: in tal caso è necessario comunicare la violazione all'interessato senza ingiustificato ritardo, a meno che non si verifichino le circostanze indicate nel paragrafo 3 dell'articolo:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Per ottemperare agli obblighi imposti dalla norma, ogni utente avvisa senza indugio i Sistemi Informativi, segnala anche al proprio Direttore/Responsabile le violazioni o gli incidenti informatici che ha rilevato e che possono avere un impatto significativo sui dati personali. Il Direttore/Responsabile dei dati avvisa i Sistemi Informativi e, unitamente, procedono alle comunicazioni dell'avvenuto incidente di databreach e all'avvio dell'istruttoria per la comunicazione all'interessato/i.

2. SEZIONE II – Password e sicurezza

2.1. Le Password

Le password sono un metodo di autenticazione assegnato dall'Università per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software.
La prima caratteristica di una password è la segretezza, cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro e a quello dei colleghi e dell'Università nel suo complesso.
Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.
L'Università ha implementato alcuni meccanismi che permettono di aiutare e supportare gli incaricati in una corretta gestione delle password; in particolare, per quanto riguarda quelle di

accesso ad ogni dispositivo utilizzato (sia fisico che online), vengono aggiornate periodicamente secondo il livello di sicurezza richiesto dall'Università e, comunque, in linea con quanto richiesto dalla normativa privacy.
Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone: il miglior luogo in cui conservare una password è la propria memoria.
Le utenze che non vengono utilizzate da parte dei responsabili per un periodo superiore ai sei mesi, verranno considerate disattivabili dall'Università.
In qualsiasi momento, l'Università si riserva il diritto di revocare all'utente il permesso di accedere ad un sistema hardware o software, a cui era precedentemente autorizzato, disabilitando l'utenza ad esso associata.

2.2. Regole per la corretta gestione delle password

L'utente, da parte sua, per una corretta e sicura gestione delle proprie password, deve 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 dubbio che sia diventata poco "*sicura*";
3. le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;
4. le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
5. le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password;
6. evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Università. In alcuni casi, sono implementati meccanismi che consentono all'utente 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 alcuni minuti. In caso di necessità, contattare i Sistemi Informativi.

2.3. Divieto di uso

Al fine di una corretta gestione delle password, l'Università stabilisce il divieto di utilizzare come propria password:

1. nome, cognome e loro parti;
2. lo username assegnato;
3. un indirizzo di posta elettronica (e-mail);
4. parole comuni (in Inglese e in Italiano);
5. date, mesi dell'anno e giorni della settimana, anche in lingua straniera;
6. parole banali e/o di facile intuizione, ad es. "pippo";
7. ripetizioni di sequenze di caratteri (es. abcabcabc);
8. una password già impiegata in precedenza.

2.4. La password nei sistemi

Ogni utente può variare la propria password di accesso a qualsiasi sistema dell'Università in modo autonomo, qualora il sistema in questione metta a disposizione degli utenti una funzionalità di questo tipo (Change password), oppure facendone richiesta ai Sistemi Informativi. La password può essere sostituita su richiesta dell'utente nel caso l'abbia dimenticata.

2.5. Autorizzazione e profilatura degli Utenti

Le credenziali di autenticazione per l'accesso ai sistemi e alle procedure dell'Università vengono assegnate dal personale dai Sistemi Informativi o da altro personale appositamente incaricato,

previa formale richiesta del Responsabile dell'unità operativa nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
Nel caso di collaboratori la preventiva richiesta, se necessario, verrà inoltrata direttamente dal responsabile della unità operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico. Lo stesso dicasi nel caso di revoca e/o trasferimento.
Sarà cura del Responsabile dell'unità operativa in cui opera l'utente chiedere ai Sistemi Informativi di assegnare e/o modificare i diritti di accesso ai sistemi, in base alle mansioni assegnate e svolte dall'utente.

2.6. Sicurezza dei server e delle applicazioni e della rete

I Sistemi Informativi, gestori di *server*, devono configurare i *server* medesimi conformemente agli standard di sicurezza e/o alle *best practices* (ad es. abilitare soltanto i servizi strettamente necessari, applicare sistematicamente le *"pacth",* ecc.).
Laddove le strutture interne all'Università si avvalgano di propri fornitori, diversi dai Sistemi Informativi, dovranno prevedere nei contratti di appalto l'obbligo di rispettare i predetti standard di sicurezza e, inoltre, dovranno prevedere clausole di "*responsabilità esterna*" e di "*amministrazione dei sistemi*", in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25.06.2009.
I Sistemi Informativi e le eventuali strutture esterne che sviluppino applicazioni informatiche devono rispettare l'approccio della "*privacy by design*", incorporando sia i principi e le misure a tutela della privacy nell'intero ciclo di vita delle applicazioni che, per le applicazioni web-based, le best practices emesse dall'Organizzazione internazionale Open Web Application Security Project (OWASP);
I Sistemi Informativi configurano la Rete Telematica dell'Università in modo contribuire alla protezione dei server, che sono collocati su sottoreti dedicate e con strumenti e livelli di protezione (ad es. *firewall, IPS, application firewall, ecc*.) adeguati in base al livello di classificazione assegnato ai dati ospitati nei server medesimi.

2.7. Gestione della disponibilità (salvataggio e ripristino dei dati)

Tutte le strutture dell'Università che hanno i server gestiti dai Sistemi Informativi prevedono una procedura di *"backup"* e *"restore"* per garantire la disponibilità dei dati, mitigando l'impatto causato da eventuali incidenti e/o errori che dovessero verificarsi nella gestione dei dati.

2.8. Gestione dei log file

Tutte le strutture dell'Università che hanno i server gestiti dai Sistemi Informativi di Ateneo, hanno attivo un sistema di raccolta delle informazioni relative all'accesso ai dati, sistemi, ed applicazioni utilizzati in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema) come modificato con successivo Provvedimento Generale del 25.06.2009.

2.9. Gestione delle caselle di posta elettronica

Fatto salvo quanto previsto in seguito circa l'utilizzo del servizio di posta elettronica dell'Università, ad ogni utente viene assegnato un determinato spazio per la memorizzazione sul server centrale di posta.
Esaurito il predetto spazio sul server, l'Utente potrà ricevere o spedire messaggi solo dopo aver liberato spazio sufficiente attraverso la cancellazione o lo "*scarico*" dei messaggi di posta.
Una copia di tutti i messaggi di posta elettronica "in arrivo" e in partenza, ancora presenti sul server, è salvata con procedure di *"backup"* a cadenza giornaliera per un periodo di 90 giorni.

Qualora l'utente "*scarichi*" sulla propria postazione di lavoro ovvero cancelli i messaggi di posta ancora presenti sul server, tali messaggi non saranno oggetto di *"backup"*. L'utente che ha provveduto a scaricare i messaggi sulla propria postazione di lavoro potrà richiedere ai Sistemi Informativi di includere nei backup la propria postazione.

3. SEZIONE III - Operazioni a protezione della postazione di lavoro

In questa sezione vengono trattate le operazioni a carico dell'incaricato o dal responsabile 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 dell'Università.

3.1. Login e Logout

Il "*Login*" è l'operazione con la quale l'utente si connette al sistema informativo dell'Università o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'account).
L'accesso alle postazioni di lavoro è gestito dall'Active Directory di Microsoft.
Per le applicazioni web, l'Università ha predisposto un unico login tramite l'accesso all'area riservata del portale Link www.unilink.it; da questa pagina è possibile accedere con un unico account.
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. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati dell'Università.
Il responsabile deve quindi eseguire le operazioni seguenti:

1. se si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti;
2. bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
3. chiudere la sessione (Logout) a fine giornata;
4. spegnere il PC dopo il Logout;
5. controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

4 SEZIONE IV - Uso del personal computer dell'Università

4.1. Modalità d'uso del computer dell'Università

Il sistema informativo dell'Università è composto da un insieme di unità (server centrali e in cloud e client) connessi ad una rete locale (LAN e/o WAN), che utilizzano diversi sistemi operativi e applicativi.
I file creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati sul proprio computer o sulle cartelle condivise. L'Università, tranne per particolari casi, non effettua il backup dei dati memorizzati in locale.

4.2. Corretto utilizzo del computer dell'Università

Il computer consegnato all'utente 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 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'utente con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'Università. Per necessità dell'Università, gli amministratori di sistema, utilizzando la propria login con privilegi di amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server dell'Università nonché, previa comunicazione all'utente, accedere al computer anche in remoto.
In particolare l'utente deve adottare le seguenti misure:

1. utilizzare solo ed esclusivamente le aree di memoria della rete dell'Università ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete;
2. spegnere il computer, o curarsi di effettuare il Logout, 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'Università;
4. non dare accesso al proprio computer ad altri utenti, a meno che siano responsabili con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

4.3. Utilizzo delle risorse condivise

Le unità di rete sono aree di condivisione di dati esclusivamente inerenti all'attività lavorativa e non possono in alcun modo essere utilizzare per scopi diversi. Pertanto:

a) qualunque informazione che non sia riferibile alla predetta attività non può essere nemmeno parzialmente (o, anche solo, temporaneamente) localizzata su dette aree;
b) le unità di rete non possono essere utilizzate per fini non espressamente autorizzati;
c) non è consentito connettere in rete postazioni di lavoro, senza la preventiva autorizzazione dei Sistemi Informativi di Ateneo;
d) è vietato condividere cartelle in rete sulla propria postazione di lavoro anche se protette da password o da un elenco incaricati autorizzati, senza preventiva richiesta da parte del responsabile della propria area di riferimento/appartenenza e autorizzazione dei Sistemi Informativi di Ateneo.

4.4. Divieti espressi sull'utilizzo del computer

All'utente è vietato:

1. gestire, memorizzare (anche temporaneamente) o trattare file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa dell'Università e negli strumenti informatici dell'Università in genere;
2. modificare le configurazioni già impostate sul personal computer;
3. utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell'Università;
4. installare alcun software di cui l'Università non possieda la licenza, né installare alcuna versione diversa, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l'espressa autorizzazione dell'Università. È, peraltro, vietato fare copia del software installato al fine di farne un uso personale;

5. caricare sul disco fisso del computer o nel server documenti, giochi, file musicali o audiovisivi o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
6. aggiungere o collegare dispositivi hardware (ad esempio hard disk, chiavi USB, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, ecc.) diversi da quelli autorizzati o consegnati, senza l'autorizzazione espressa dell'Università;
7. creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'Università, quali per esempio virus, trojan horses e malware in genere;
8. accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte;
9. effettuare in proprio attività manutentive;
10. permettere attività manutentive da parte dei soggetti non espressamente autorizzati dell'Università.

4.5. Antivirus

I virus (o, per essere precisi, il malware, il software malevolo) possono essere trasmessi tramite scambio di file via internet, via email, scambio di supporti removibili, filesharing, chat, ecc.
L'Università impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.
L'utente, da parte sua, deve impegnarsi 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'Università ogni anomalia o malfunzionamento del sistema antivirus;
2. comunicare all'Università eventuali segnalazioni di presenza di virus o di file sospetti.

Inoltre, all'utente:

1. è vietato accedere alla rete dell'Università senza servizio antivirus attivo e aggiornato sulla propria postazione;
2. è vietato ostacolare l'azione dell'antivirus dell'Università;
3. è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Università, anche e soprattutto nel caso in cui sia richiesto per l'installazione di software sul computer;
4. è vietato aprire allegati di email provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di email di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i Sistemi Informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

5 SEZIONE V - Internet

5.1. Internet è uno strumento di lavoro

La connessione alla rete internet dal dispositivo avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa. L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.
In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

5.2. Misure preventive per ridurre navigazioni illecite

L'Università adotta idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all'attività lavorativa attraverso filtri e black list.
I siti accessibili agli utenti dipendono dal profilo di navigazione assegnato. Un eventuale cambio di profilo di navigazione, se necessario, può essere richiesto direttamente dal responsabile della unità operativa con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

5.3. Divieti espressi concernenti Internet

- È fatto divieto di 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;
- è vietato all'utente lo scarico (download) di software (anche gratuito) prelevato da siti Internet;
- è tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti online e simili, salvo i casi direttamente autorizzati dal Responsabile dell'ufficio di appartenenza e con il rispetto delle normali procedure di acquisto;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- è vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche; anche partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'Università, salvo specifica autorizzazione della stessa;
- è vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- è vietato all'utente di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica dell'Università;
- è vietato creare siti web personali sui sistemi dell'Università, nonché acquistare beni o servizi su Internet, a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione che comporti un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e particolari, è posta sotto la personale responsabilità dell'utente inadempiente.

5.4. Divieti di Sabotaggio

È vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'Università per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

5.5. 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 (es. legge 22 aprile 1941, n. 633 e successive modificazioni, D. Lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, ...) se non espressamente autorizzato dall'Università.

6 SEZIONE VI - Posta elettronica

6.1. La Posta Elettronica è uno strumento di lavoro

L'utilizzo della posta elettronica dell'Università è connesso allo svolgimento dell'attività lavorativa. L'uso per motivi personali deve essere moderato ed è tollerato esclusivamente ai sensi dell'articolo seguente. Gli utenti hanno in utilizzo indirizzi nominativi di posta elettronica.

Le caselle e-mail possono essere assegnate anche con natura impersonale (tipo info, amministrazione, fornitori, direttore, collaboratore, consulenza, ...). Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

6.2. Misure preventive per ridurre utilizzi illeciti della Posta Elettronica

L'Università è consapevole della possibilità di un limitato utilizzo personale della posta elettronica da parte degli utenti e allo scopo prevede le seguenti misure:

1. in caso di ricezione sulla email dell'Università di posta personale, si chiede di cancellare immediatamente questi tipi di messaggio;
2. avvisare l'Università quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta.

6.3. Divieti espressi

1. È vietato utilizzare l'indirizzo di posta elettronica contenente il nome di dominio dell'Università per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa l'autorizzazione della stessa, nonché utilizzare il dominio dell'Università per scopi personali;
2. è fortemente consigliato scrivere e generare messaggi di posta elettronica con l'indirizzo dell'Università, diretti a destinatari esterni, utilizzando la seguente dichiarazione:
   "*Il presente messaggio e gli eventuali suoi allegati sono di natura dell'Università, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'Università oltre al sottoscritto, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività dell'Università. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente*";
3. è vietato creare, archiviare o spedire, anche solo all'interno della rete dell'Università, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, "*catene di Sant'Antonio*" o in genere a pubblici dibattiti utilizzando l'indirizzo dell'Università;
4. è vietato trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria;
5. è vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro;
6. è vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'Università informazioni riservate o comunque documenti dell'Università, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;
7. è vietato utilizzare la posta elettronica per messaggi con allegati di grandi dimensioni. La dimensione degli allegati non deve superare i 20 MB.

Le condizioni di utilizzo della casella di posta elettronica assegnata, fissate dall'Università, sono le seguenti:

a. *finalità del servizio di posta elettronica*. L'Università incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro;
b. *proprietà dell'Università*. Il servizio di posta elettronica, erogato dai propri server, è proprietà dell'Università, pertanto ogni casella di posta elettronica nel dominio associata ai suoi uffici o assegnata a individui o funzioni, sono di proprietà dell'Università;
c. *limitazioni di responsabilità*. L'Università non può essere ritenuta responsabile per qualsiasi danno, diretto o indiretto, arrecato all'utente ovvero a terzi e derivante: - dall'eventuale interruzione del servizio - dall'eventuale smarrimento di messaggi diffusi per mezzo del servizio - da messaggi inviati/ricevuti o da transazioni eseguite tramite il servizio - da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'utente;

d. *restrizioni all'uso del servizio*. Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè rispettando le leggi, la presente e altre politiche e procedure dell'Università e secondo i normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica può essere totalmente o parzialmente limitato dall'Università, senza necessità di assenso da parte dell'utente e anche senza preavviso: quando richiesto dalla legge e in conformità ad essa, nel caso di comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti, al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Università) e, in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili;
e. *disattivazione*. L'accesso ai servizi di posta elettronica può essere disattivato dall'Università in caso di cessazione del rapporto di lavoro o di non utilizzo della stessa per un periodo superiore ai 6 mesi, senza necessità di assenso da parte dell'utente. Non è prevista alcuna forma di indennizzo per il venir meno del servizio;
f. *assenso e conformità*. L'Università è tenuta in generale ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o per l'accesso alle registrazioni o ai messaggi di posta elettronica. D'altro canto, ci si attende che l'utente soddisfi le richieste dell'Università riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso che riguardino le attività lavorative o richieste per soddisfare gli obblighi di legge. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui la punto e);
g. *limitazioni all'accesso senza assenso*. L'Università non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. D'altro canto, l'Università potrà permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, solamente nei seguenti casi:
    - su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente;
    - previo preavviso all'utente, per gravi e comprovati motivi, che facciano credere che siano state violate le disposizioni di legge vigenti o le politiche dell'Università in materia di sicurezza;
    - per atti dovuti;
    - in situazioni critiche e di emergenza;
h. *limitazioni all'accesso senza assenso*. L'Università non ispeziona e non accede ai messaggi di registrazione elettronica. L'Università registra e conserva i dati, delle caselle di posta elettronica messe a disposizione dei propri utenti tramite scrittura in appositi file di log, delle seguenti informazioni minime per ogni messaggio:
    - mittente;
    - destinatario/i;
    - giorno ed ora dell'invio;
    - esito dell'invio.

I file di registro sono conservati per un periodo di 2 (due) anni.

6.3.1. Avvertenze

Gli utenti del servizio di posta elettronica sono avvisati del fatto che:

1. la natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. L'Università non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o dati sensibili;
2. i messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Università che su altri sistemi, possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. È possibile quindi che venga richiesto di

accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Università. L'Università non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la normativa privacy ed altre normative applicabili. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Università può garantire che non saranno accedute informazioni personali degli utenti presenti in messaggi di posta elettronica residenti sui propri sistemi;

3. l'Università, in generale, non può e non intende porsi come valutatore dei contenuti dei messaggi di email scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di cortesia che adopererebbero in altre forme di comunicazione;
4. non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto, perché è piuttosto semplice per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione della presente politica. Inoltre i messaggi di posta che arrivano come "*inoltro*" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica dovrebbe sempre verificare con il mittente l'autenticità delle informazioni ricevute.

6.3.2. Uso consentito

L'uso del servizio di posta elettronica dell'Università è soggetto alle seguenti condizioni:

a. *proibizioni*. È fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione dell'Università. È inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli utenti del servizio. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi email che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo ai Sistemi Informativi utilizzando i servizi di assistenza;
b. *uso personale*. È consentito l'utilizzo del proprio account nel dominio a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non:
   - sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Università;
   - sia causa di oneri aggiuntivi per l'Università;
   - interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Università.

L'utente è edotto del fatto che l'Università considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. L'Università presuppone quindi che quell'utente che decide di utilizzare la posta elettronica per scopi personali, ne ha preliminarmente e attentamente valutato l'opportunità. Si ricorda comunque che per gli usi personali è possibile dotarsi di una casella di posta elettronica alternativa, ottenibile gratuitamente presso molti fornitori esterni, e liberamente consultabile via internet.

6.3.3. Sicurezza e riservatezza

Oltre a quanto indicato ai paragrafi precedenti, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è

possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora di verificassero i casi citati.
L'Università si pone come obiettivo fondamentale la fornitura di servizi di posta elettronica sicuri ed affidabili; ma va comunque ricordato che, come già detto in precedenza, tale sicurezza e riservatezza non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui personal computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni e alla propria postazione di lavoro.

6.4. Posta Elettronica in caso di assenze programmate ed assenze non programmate

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (auto-reply).
In alternativa, e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività dell'Università, l'utente deve nominare un collega fiduciario che in caso di assenza inoltri i file necessari a chi ne abbia urgenza.
Qualora l'utente non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'Università, mediante personale appositamente responsabile, potrà verificare il contenuto dei messaggi di posta elettronica dell'utente, informandolo.

6.5. Utilizzo illecito della Posta Elettronica

È vietato inviare, tramite la posta elettronica, anche all'interno della rete dell'Università, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico.
È vietato inviare messaggi di posta elettronica, anche all'interno della rete dell'Università, 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.
Qualora un utente riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'Università.

7 SEZIONE VII - Uso di altri dispositivi

(Notebook, tablet, cellulare, smartphone e di altri dispositivi elettronici)

7.1. L'utilizzo del notebook, tablet o smartphone.

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "*dispositivi mobili*") possono venire concessi in uso dall'Università agli incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete.
L'utente è responsabile dei dispositivi mobili assegnatigli dall'Università e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
I notebook e i tablet mobili dell'Università, concessi in uso, possono essere connessi alla rete wifi dell'Università protetta. Questa attività potrà avvenire dopo esplicita richiesta ai Sistemi Informativi, dovrà essere autorizzata e sarà svolta dal personale dei Sistemi Informativi.
Ai dispositivi 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.
In particolare i file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa dell'Università al primo rientro in ufficio e cancellati in modo definitivo dai dispositivi mobili (*Wiping*). Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non

espressamente autorizzate dall'Università. I dispositivi mobili utilizzati all'esterno (convegni, visite in Università, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili, deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Università che provvederà, se del caso, ad occuparsi delle procedure connesse alla privacy.
All'utente è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.
I dispositivi 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 privi di PIN.
Laddove il dispositivo mobile sia accompagnato da un'utenza fonia-dati, l'utente è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, ...) e a rispettarli.
In relazione alle utenze mobili, salvo autorizzazione dell'Università, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione gli utilizzi devono essere preventivamente comunicati alla stessa per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

7.2. Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)

Agli incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, ...) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ...).
Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnati a terzi.

7.3. Dispositivi personali (BYOD).

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali se non per le finalità descritte di seguito.
Dispositivi dell'università ammessi: qualsiasi computer portatile, tablet, e-reader, smartphone. Questi dispositivi possono collegarsi alla rete wifi hotspot dell'Università presente nelle sedi dell'Università proprio per permettere agli utenti l'accesso alla sola rete internet. Il profilo di navigazione Internet è impostato e non può essere modificato.
I dispositivi personali non possono essere collegati alla rete dell'Università né in modalità wifi che con cavo di rete.

- I dispositivi possono essere usati per scopi didattici o professionali.
- È vietato agli studenti ed al personale usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto, senza il consenso esplicito dell'interessato, e solo dopo che ci sia un'autorizzazione dell'Università.
- Le credenziali per l'accesso alla rete wifi vengono consegnate dalla segreteria dell'Università all'interessato ed hanno una durata massima di 5 giorni. Queste dovranno essere conservate in modo sicuro con l'obbligo di non diffonderle a terzi.
- Per particolari esigenze didattiche o professionali si può richiedere che le credenziali siano prorogate per un tempo non superiore ad un anno. La richiesta dovrà essere approvata dal responsabile della propria area di riferimento/appartenenza.

Gli utenti non dipendenti/collaboratori (ovvero i consulenti esterni, ospiti, ecc), possono utilizzare i propri dispositivi personali e collegarsi alla rete wifi hotspot dopo aver richiesto le credenziali al personale incaricato al rilascio delle stesse.

7.4. Utilizzo del cellulare/smartphone personale.

Durante l'orario di lavoro, comprese le eventuali pause, agli incaricati e ai responsabili è concesso l'utilizzo del telefono cellulare personale, ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.
In caso di trasferte lavorative all'esterno degli uffici dell'Università, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con la stessa, ove fosse necessario.

7.5. Distruzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli incaricati o ai responsabili, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Università, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.
In particolare, l'Università provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

8 SEZIONE VIII- Sistemi in Cloud

8.1. Cloud Computing

In informatica con il termine inglese cloud computing (in italiano nuvola informatica) 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 apposta per l'utente, ma gli sono 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.
Utilizzare un servizio di cloud computing per memorizzare dati personali o particolari, espone l'Università a potenziali problemi di violazione della privacy. I dati personali vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'Università. 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. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'Università, con la difficoltà a rivalersi sul fornitore se questi risiede in uno stato diverso dal paese dell'utente.

8.2. Utilizzo di sistemi cloud

È vietato agli incaricati e ai responsabili l'utilizzo di sistemi cloud non espressamente approvati dall'Università. Per essere approvati, i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- essere sistemi cloud esclusivi e non condivisi;
- l'azienda che ufficialmente e formalmente fornisce il sistema in cloud dev'essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'Università così da garantire che tutte le indicazioni e prescrizioni previste dal GDPR (art. 20).

SEZIONE IX - Gestione dati cartacei

9.1. Clear Desk Policy

Tutti gli utenti sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
Gli utenti sono invitati dall'Università ad adottare una "*politica della scrivania pulita*". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dall'Università.
I principali benefici di una politica della scrivania pulita sono:

- una buona impressione a clienti e fornitori che visitano la nostra organizzazione;
- la riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- la riduzione del rischio che documenti confidenziali possano essere sottratti all'Università.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa, oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.
Prima di lasciare la propria postazione, sarà cura degli incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, ...) i dati cartacei a loro affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'Università.
A fine giornata, dev'essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.
Ove possibile, s'invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.
Ove possibile, s'invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.
Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

10 SEZIONE X - Applicazione e controllo

10.1 Il controllo

L'Università, 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:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo;
- 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'Università si riserva di avvalersi anche di soggetti esterni.
Si precisa, in ogni caso, che l'Università non adotta "*apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

10.2. Modalità di verifica

In applicazione del principio di necessità di cui all'art. 3 del Codice Privacy, l'Università promuove ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "*minimizzare*" l'uso di dati riferibili agli incaricati; allo scopo, ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Università non adotta 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 degli incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.
Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di file pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

10.3. Modalità di Conservazione

I sistemi software che regolano gli accessi ad Internet e al traffico telematico sono gestiti dall'Università, la quale garantisce che i dati, la cui conservazione non è necessaria, non sono conservati o sono cancellati periodicamente o automaticamente.
Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'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 e sarà effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

11 SEZIONE XI- Soggetti preposti del trattamento, responsabili e responsabili

11.1. Individuazione dei Soggetti autorizzati

L'Università ha designato un Responsabile del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

Tutti i dipendenti e i collaboratori risultano essere soggetti autorizzati al trattamento dei dati in funzione del modulo "*Individuazione scritta della persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art.28 par. 3, lett. b), Reg. UE 2016/679*)" accettato e controfirmato al momento della sottoscrizione del contratto.
Per quanto riguarda i soggetti designati come Amministratori di sistema, con il relativo modulo accettato e controfirmato al momento della sottoscrizione del contratto, possono svolgere solo operazioni strettamente necessarie al perseguimento delle finalità di sicurezza informatica, senza poter svolgere attività di controllo a distanza, neanche di propria iniziativa.

12 SEZIONE XII - Provvedimenti Disciplinari

12.1. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente regolamento potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge e/o del Contratto Collettivo Nazionale del Lavoro applicato, tra cui:

- il biasimo inflitto verbalmente;

- la lettera di richiamo inflitta per iscritto;
- una multa;
- la sospensione temporanea dalla retribuzione e dal servizio;
- il licenziamento disciplinare, con le altre conseguenze di ragioni e di legge.

Per i dirigenti valgono le vigenti norme di legge e/o di contrattazione collettiva, fermo restando che, per le violazioni di maggior gravità, l'Amministrazione potrà procedere al licenziamento del dirigente autore dell'infrazione.

12.2. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto ad accedere, ai sensi dell'art. 15 del Regolamento, alle informazioni che lo riguardano scrivendo al Titolare dell'Università.

13 SEZIONE XIII - Validità, Aggiornamento ed Affissione

13.1. Validità

Il presente Regolamento ha validità a partire dal giorno successivo all'emanazione.

13.2. Aggiornamento

Il presente Regolamento sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'Università o in caso di mutazioni legislative.
Ogni variazione del presente regolamento sarà comunicata agli interessati.

13.3. Affissione

Il presente regolamento è pubblicato sul Portale Istituzionale dell'Università degli Studi Link (Area Riservata).