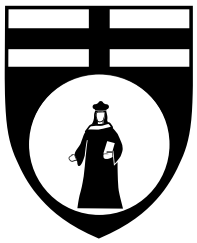

Università
di Genova

Linea Guida ICT

Sicurezza informatica

Versione	Autori
Ottobre 2024	Stefano Orocchi (Area ICT) Massimo Di Spigno (Area ICT)

Sommario

Introduzione

L'Università degli Studi di Genova, a cui ci si riferisce in seguito come Unige, o Ateneo, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli strumenti informatici dell'Ateneo da parte dei dipendenti, degli studenti e di tutti coloro che, in virtù di un rapporto di lavoro, di studio, o di ricerca, a qualsiasi titolo (collaboratori, consulenti, stagisti, fornitori, studenti esterni, etc.), utilizzano strumenti informatici dell'Ateneo, nel seguito denominati Utenti.

Il presente documento deve considerarsi integrato da tutte le procedure interne adottate per argomenti specifici e casistiche, così come pubblicati sul sito dell'Ateneo e più specificatamente dell'Area ICT.

Finalità del documento

Il presente documento definisce e detta agli Utenti specifiche regole e condizioni di utilizzo degli strumenti informatici aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree operative e Strutture organizzative;
- definizione di regole e procedure attinenti a specifici ambiti di applicazione;
- indicazione del corretto approccio da seguire in assenza di regole specifiche per una determinata specifica casistica;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- definizione dell'ambito, delle modalità, dei limiti del monitoraggio e dei controlli attuabili dall'Ateneo nel rispetto della normativa vigente nonché delle regole e delle procedure interne.

Contesto normativo e regolamentare

Il presente regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8 e successive modificazioni;
- D. Lgs. 196/2003 e s.m.i(Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento Unige;

- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1417809
- REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
- DECRETO LEGISLATIVO 4 settembre 2024, n. 134 (recepimento NIS 2) - Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. (24G00150) (GU Serie Generale n.223 del 23-09-2024)
- Piano Implementativo Strategia Nazionale Cybersicurezza 2022-2026
- Piano Triennale per l'informatica nella PA

GLOSSARIO E DEFINIZIONI

Ai fini del presente documento si intende per:

- Amministratori di sistema: figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate in conformità al Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;
- Applicazioni aziendali: si considerano applicazioni aziendali:
    - Prodotti/programmi acquistati dall'Ateneo, di valenza generale, o settoriale ed in quest'ultimo caso approvati dall'Area ICT;
    - Applicazioni e servizi sviluppati ad hoc dell'Area ICT, da terze parti ma sotto il coordinamento dell'Area ICT, ovvero da altre strutture con un processo di partecipazione e approvazione da parte dell'Area ICT e che seguono le regole di gestione previste nei casi precedenti;
    - Applicazioni esterne che l'Ateneo utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma NoiPA, abbonamenti a servizi informativi, portale ANAC, etc.
- Aziendali: nel corso del documento si farà spesso riferimento a risorse o dispositivi come "aziendali". Pur nella consapevolezza che l'Ateneo non è un'azienda, tale dicitura identifica più chiaramente l'organizzazione nella letteratura tecnica.
- Dispositivi o endpoint: qualunque dispositivo atto a connettersi alla rete Unige, ai suoi dati, alle applicazioni aziendali, alle risorse in genere.
- Dispositivi aziendali: dispositivi di proprietà o comunque nelle disponibilità dell'Università degli studi di Genova e messi nelle disponibilità degli utenti.
- File di log: registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- GENUAnet: rete informatica gestita direttamente dall'Università di Genova divisa in rete cablata e rete WiFi eduRoam (già GenuaWiFi);
- Strumenti informatici: personal computer fissi o portatili o virtuali, stampanti locali o di rete, programmi e prodotti software in-house o in-cloud, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- Utenti: personale dipendente, docenti, studenti, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto di lavoro, di studio o di collaborazione in essere a qualsiasi titolo con l'Ateneo, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione da Unige.

PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività e devono essere utilizzati con modalità e mediante comportamenti adeguati al ruolo, ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne e delle leggi.

Nell'esecuzione della propria attività, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a. effettuare la propria attività uniformandosi alle disposizioni dell'Ateneo e alle istruzioni ricevute;
b. custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c. mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;
d. in caso di cessazione dal servizio, dalla prestazione o dal rapporto con l'Ateneo, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività, in funzione della natura di riservatezza del dato;
e. adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
f. garantire la corretta custodia di atti e documenti adottati da Unige.

REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI DI ATENEO

Credenziali di autenticazione

L'accesso alle applicazioni del sistema informativo di Ateneo avviene attraverso credenziali di autenticazione centralizzate fornite e gestite dall'Area ICT (es. credenziali Unigepass, credenziali Cloud), o tramite sistemi di autenticazione esterni autorizzati dall'Area ICT (es. SPID). L'accesso a particolari dispositivi, servizi o applicazioni può avvenire tramite credenziali locali in accordo l'Area ICT (es. particolari allestimenti di laboratorio).

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato.

Il sistema di controllo degli accessi implementa regole che seguono l'evoluzione della tecnologica e delle necessità di sicurezza.

I dettagli dei requisiti richiesti per l'utilizzo dell'autenticazione sono disponibili sulle pagine del web di ateneo e più specificatamente nelle pagine dell'Area ICT.

Utilizzo di applicazioni aziendali

L'accesso alle applicazioni aziendali e il loro utilizzo devono avvenire secondo le regole del presente documento e sulla base del ruolo ricoperto dall'utente e le relative responsabilità e regole ad esse conseguenti.

L'accesso alle applicazioni aziendali deve essere finalizzato allo svolgimento del proprio ruolo in Ateneo e non presentare conflitto con esso.

Il ruolo di un Utente in Ateneo e le attività ad esso legate determinano le autorizzazioni all'accesso alle risorse aziendali. Tali autorizzazioni vengono assegnate dai sistemi informativi con l'applicazione di automatismi e richiedono quindi la costante disponibilità di dati quanto più possibile esatti nei sistemi informativi dell'Ateneo.

L'accesso alle applicazioni aziendali può avvenire tramite:

- dispositivi aziendali, allestiti da, per conto, con l'assenso dell'Area ICT.
- dispositivi di proprietà o nelle disponibilità dell'utente, caso definito anche di Bring Your Own Device (BYOD)

In ogni caso, l'accesso alle applicazioni e alle risorse aziendali segue le stesse regole e raccomandazioni per quanto concerne la sicurezza e le modalità di accesso e utilizzo, così come descritto nel presente documento.

L'Area ICT sovrintende alle corrette modalità di accesso e utilizzo delle applicazioni e risorse aziendali anche in modo delegato, provvede a dare informazione all'Ateneo dei corretti modi di utilizzo delle risorse informative aziendali, a formare gli Utenti e il personale eventualmente delegato in Ateneo.

L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni.

L'accesso alle applicazioni aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità di accesso alle risorse aziendali può cessare o andarsi a modificare, solitamente in modo automatico. L'utente è tenuto a mantenersi informato dei corretti criteri di accesso ai programmi e delle risorse di cui ha disponibilità.

Utilizzo di dispositivi aziendali

I dispositivi aziendali vengono preparati e gestiti da, per conto, con l'assenso dell'Area ICT secondo regole che evolvono con il progredire delle tecnologie e delle minacce informatiche. Ne è vietato qualunque utilizzo che danneggi le risorse aziendali (es. il dispositivo stesso, o il software, o i dati), o che sia di minaccia per la sicurezza. È consentito l'uso promiscuo, sia lavorativo, sia personale, del dispositivo, purché non contraddica alcuna altra regola del presente documento, o dell'Ateneo.

Il dispositivo è provvisto di software di sicurezza (es. antivirus, firewall, impostazioni di aggiornamento) e le configurazioni disposte o raccomandate seguono regole come descritte nel presente documento e altre linee guida opportunamente fornite dall'Area ICT.

Nei casi in cui l'Utente, o comunque altro personale opportunamente delegato, dispongano di diritti amministrativi sul dispositivo, dovranno assicurarsi in prima persona della corretta configurazione e mantenimento del dispositivo ed evitare comportamenti diversi dalle raccomandazioni.

Nei casi in cui l'utente, o comunque altro personale opportunamente delegato, abbiano autonomia di installazione/utilizzo di applicazioni, anche senza diritti amministrativi, dovranno assicurarsi in prima persona della corretta configurazione e mantenimento di esse ed evitare comportamenti diversi dalle raccomandazioni.

In caso di dubbio sul comportamento da seguire (es. l'installazione di un programma non aziendale), l'utente, o comunque altro personale opportunamente delegato, dovranno consultare il personale dell'Area ICT prima di procedere.

L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, il ritiro del dispositivo affidato, o anche procedure legali ove necessario.

Tra i dispositivi aziendali rientrano anche i dispositivi e le risorse virtuali. Le regole di cui al presente documento valgono anche per essi per quanto applicabile.

L'accesso ai dispositivi aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità dei dispositivi aziendali può cessare o andarsi a modificare. L'utente è tenuto a informarsi dei corretti criteri di detenzione e restituzione dei dispositivi in affidamento.

Utilizzo di dispositivi non aziendali

L'accesso alle risorse aziendali può avvenire tramite dispositivi diversi da quelli aziendali, ad esempio di proprietà o nelle disponibilità dell'utente, oppure di accesso pubblico. Le norme comportamentali per l'utente restano invariate. L'utente si fa responsabile in prima persona nell'accesso alle risorse aziendali di utilizzare dispositivi sicuri, a norma di legge, secondo il regolamento di Ateneo (es. software installato aggiornato, presenza di antivirus e firewall correttamente funzionanti, nessuna minaccia locale rilevata).

L'accesso a risorse aziendali su dispositivi personali prevede un analogo trattamento in termini di assistenza all'utilizzo, ma che non si estende al dispositivo stesso, a cura invece dell'utente.

L'accesso alle applicazioni aziendali è legato al ruolo dell'utente in Ateneo. Al modificarsi, o al termine del ruolo dell'utente in Ateneo, la disponibilità di accesso alle risorse aziendali può cessare o andarsi a modificare, solitamente in modo automatico. L'utente è tenuto a mantenersi informato dei corretti criteri di accesso ai programmi e delle risorse di cui ha disponibilità e delle ripercussioni sul proprio dispositivo del venire a mancare delle risorse aziendali.

Configurazioni speciali dei dispositivi

In casi eccezionali può verificarsi la necessità di tenere in esercizio dispositivi che potrebbero violare alcune norme del presente o altri regolamenti. Un esempio può essere dato dal caso di particolari insostituibili attrezzature per l'acquisizione per i quali sussistano problemi tecnici di incompatibilità con i moderni computer. Questi casi devono essere discussi preventivamente con l'Area ICT, così di concordare un modello di allestimento che non pregiudichi la sicurezza delle risorse aziendali. Il parere dell'Area ICT in materia è vincolante.

Accesso alla rete

L'accesso alla rete internet è messo a disposizione degli utenti per le finalità di lavoro, ricerca, didattica, utili per lo svolgimento del proprio ruolo in Ateneo.

Qualsiasi operazione effettuata sulla rete interna o esterna all'ateneo (accesso a siti web per necessità inerenti e non l'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è

sotto la responsabilità dell'utente che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome dell'Ateneo.

Ogni Utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare la rete per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- trasferire sul proprio computer (download) solo file da siti web verificati e affidabili, tenendo presente che, quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine dell'Ateneo e dei colleghi;
- la navigazione in rete avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali; in ogni caso è vietato accedere a siti i cui contenuti non siano adeguati all'immagine e al buon nome dell'Ateneo.

Al fine di prevenire l'accesso a siti e risorse potenzialmente nocivi, l'Area ICT adotta soluzioni di sicurezza che possono monitorare e bloccare l'accesso a risorse potenzialmente pericolose o dai contenuti illeciti. Sono adottate tecnologie anti-malware che permettono la scansione della navigazione, prevenendo lo scaricamento del contenuto malevolo.

Gi strumenti predisposti dall'Area ICT, richiedono parimenti un corretto e responsabile comportamento da parte dell'utente.

Posta elettronica

Gli utenti sono dotati di un indirizzo di posta elettronica sui sistemi di Ateneo. I sistemi di posta di Ateneo si compongono di risorse informatiche hardware e software gestite direttamente dall'Area ICT (insieme dei Server on-premise e cloud Exchange Online) a cui ci si riferirà come "posta di ateneo", o "posta Unige". L'Area ICT gestisce e supervisiona il sistema di posta garantendo il corretto flusso documentale e monitorando l'utilizzo corretto da parte degli utenti, nonché la sicurezza del sistema nel suo insieme.

In aggiunta a questi sistemi, sono presenti in ateneo sistemi di posta gestiti autonomamente da strutture/dipartimenti con l'accordo e il monitoraggio dell'Area ICT, per motivazioni funzionali e subordinatamente alla regolamentazione e supervisione dell'Area ICT.

Le modalità di attribuzione e gestione delle caselle di posta di ateneo sono regolamentate dalla policy sulla posta elettronica emanata dall'Area ICT.

Ad ogni utente viene assegnato un indirizzo di posta elettronica sulla posta di ateneo che costituisce il suo indirizzo e-mail principale di lavoro e che viene pubblicato nelle rubriche di Ateneo. Ad esso possono essere affiancati alias ritenuti funzionalmente opportuni. Tale indirizzo corrisponde solitamente anche all'UPN, login sul sistema di autenticazione di Ateneo e quindi su una molteplicità di applicazioni aziendali.

Gli indirizzi di posta, le caselle di archiviazione, quando associate, e tutti gli aspetti inerenti al sistema di posta vengono gestiti dall'Area ICT nell'osservanza della policy relativa e sulla base delle necessità di sicurezza e tecniche.

Il sistema di posta di Ateneo deve essere utilizzato esclusivamente per l'esercizio della propria attività all'interno dell'Ateneo, in funzione del proprio ruolo. È da evitarne l'utilizzo per fini personali (es. domiciliazione bollette private).

I sistemi di posta esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

Sono previste caselle di posta condivise per agevolare la condivisione del lavoro di gruppo. L'assegnazione e la gestione di queste caselle segue la policy sulla posta elettronica emanata dall'Area ICT.

Nell'utilizzo della posta elettronica è necessario osservare comportamenti consoni. In particolare, si ricorda l'obbligo di:

- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine dell'Ateneo o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- Prestare la massima attenzione per evitare di cadere vittima di fishing o di altri attacchi informatici, soprattutto quando di natura nota e riconoscibile;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi o a liste di distribuzione interne all'Ateneo, salvo motivata e lecita necessità;
- evitare l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
- evitare di diffondere, all'esterno dell'Ateneo, indirizzi di posta elettronica di altri utenti, per motivi non legati all'attività lavorativa.

Valgono per la posta elettronica tutti gli obblighi e le raccomandazioni inerenti al trattamento dei documenti e dei dati in genere.

Servizi di comunicazione (chat, messaggistica, videoconferenza, telefonia)

Gli strumenti di comunicazione, oltre alla posta elettronica, comprendono la chat, la telefonia, la videoconferenza e la collaborazione sui documenti. Ciascuno di questi strumenti, di natura diversa tra loro, viene gestito in maniera armonizzata dall'Area ICT, o sotto la sua supervisione.

Gli strumenti messi a disposizione dall'Ateneo e amministrati dall'Area ICT consentono lo svolgimento delle attività in Unige in osservanza delle leggi e dei regolamenti vigenti. Gli strumenti informatici in uso sono rispondenti ai requisiti stringenti in merito al trattamento dell'informazione e anche la loro amministrazione interna all'Ateneo, di cui è responsabile

l'Area ICT, permette di garantire la riservatezza dei documenti e l'osservanza dei dettami di legge tramite un lavoro di continuo monitoraggio e adeguamento. Viene scoraggiato l'utilizzo di sistemi di comunicazione diversi da quelli gestiti o raccomandati dall'Area ICT.

Durante l'utilizzo di tali strumenti è opportuno adottare comportamenti consoni, come da relativi regolamenti e rispettare le indicazioni fornite dall'Area ICT in materia di adozione degli strumenti e loro modalità di utilizzo.

Si raccomanda di utilizzare in maniera congrua lo strumento di segnalazione del proprio stato di occupazione (libero, in riunione, non disturbare, etc,) in quelle applicazioni che lo permettono (es. Teams, Outlook). Si raccomanda di osservare lo stato di disponibilità di un altro utente prima di tentare di chiamarlo, se disponibile, così da non interrompere altre attività in corso, o abusare del tempo della controparte quando fuori servizio.

Nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa unionale e nazionale in materia di protezione dei dati personali, sono attivi sistemi di monitoraggio delle comunicazioni che consentono di verificare mittente, destinatario, durata/data e stato. Detti sistemi sono destinati esclusivamente all'analisi del tipo di traffico ai fini di reportistica e manutenzione e le relative informazioni (dati aggregati) sono accessibili ai soli amministratori dei sistemi di comunicazione.

Nell'utilizzo sistemi di comunicazione è necessario osservare comportamenti consoni. In particolare, si ricorda l'obbligo di:

- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- assicurarsi che sia evidente a tutti i partecipanti a una comunicazione l'inizio e il termine di una registrazione;
- evitare di diffondere il contenuto di una comunicazione in maniera non concordata con gli altri interlocutori, soprattutto se in presenza di contenuti riservati o sensibili;
- evitare l'utilizzo di linguaggi ingiuriosi, minatori, lesivi dell'immagine dell'Ateneo o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di persone interne o esterne all'Ateneo, salvo motivata e lecita necessità;
- evitare di diffondere, all'esterno dell'Ateneo, indirizzi di posta elettronica di altri utenti, per motivi non legati all'attività lavorativa.

Archiviazione, condivisione e servizi Cloud

L'archiviazione aziendale dell'ateneo si compone dell'insieme delle capacità di archiviazione *on-premise* e sul cloud che vanno a comporre complessivamente il sistema di archiviazione di Unige.

Rispetto alla capacità di archiviazione dei dispositivi, l'archiviazione aziendale permette una maggiore sicurezza del dato, resilienza ai guasti e possibilità di monitoraggio da parte degli amministratori di sistema. La legge obbliga l'Ateneo nel suo insieme e ogni suo utente singolarmente a custodire con cura l'informazione di cui è responsabile. Gli strumenti messi a

disposizione dall'Ateneo per la gestione documentale personale e di gruppo agevolano questo compito e sono stati individuati come adeguati a tale scopo dall'Area ICT.

I sistemi di archiviazione di Ateneo si compongono di risorse informatiche hardware e software gestite direttamente dall'Area ICT o sotto suo mandato (insieme dei file server on-premise e cloud Sharepoint Online, OneDrive, Titulus, etc.) a cui ci si riferirà come "archiviazione di ateneo".

Il sistema di archiviazione di Ateneo deve essere utilizzato esclusivamente per l'esercizio della propria attività all'interno dell'Ateneo, in funzione del proprio ruolo. È da evitarne l'utilizzo per fini personali (es. documenti personali, foto, filmati).

I sistemi documentali esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

L'archiviazione di Ateneo viene gestita e monitorata dall'Area ICT che si fa carico di indicare agli utenti i modi più consoni al suo utilizzo, nell'interesse dell'Ateneo, dei lavoratori, degli utenti in generale. A tal proposito, si sottolinea la raccomandazione di tenere sincronizzati/depositati/copiati i dati di lavoro su sistemi come OneDrive, Sharepoint, Teams o Titulus, o altri raccomandati dall'Area ICT per preservarli dalla perdita in seguito a guasti ai dispositivi personali.

In caso di comprovata necessità, gli amministratori dei sistemi si faranno carico di accedere ai sistemi di archiviazione per intervenire come necessario (es. rimozione minacce informatiche, litigation hold, etc.). L'attività degli amministratori viene svolta sempre nel rispetto della normativa in materia di tutela della libertà e dignità dei lavoratori e della normativa unionale e nazionale in materia di protezione dei dati personali.

Dispositivi di memorizzazione removibili e archiviazione locale

L'utilizzo di dispositivi removibili, utili per esempio per effettuare copie di sicurezza o per il trasporto di file di grandi dimensioni, rimane sotto la responsabilità dell'utilizzatore e va considerato sulla base dell'utilizzo previsto, della natura dei dati che deve contenere e della sicurezza con cui questo possa avvenire (utilizzo di crittografia ad es.).

In modo analogo, l'utilizzo dispositivi di archiviazione e condivisione locali come nas o piccoli server di zona, va considerato sulla base delle necessità e deve avvenire solo dopo la valutazione congiunta e il consenso dell'Area ICT.

Salvo casi particolari, questi sistemi di archiviazione non sono da considerarsi sostitutivi del sistema di archiviazione di Ateneo, ma possono essere utili come integrazione.

La conservazione di questi dispositivi implica la responsabilità diretta dell'utente che deve peraltro evitare e segnalare tempestivamente qualunque possibile smarrimento e compromissione.

Archiviazione su cloud esterni

I sistemi documentali esterni alla gestione dell'Area ICT non devono essere utilizzati per lo svolgimento di attività di Unige, salvo esplicita, motivata e circostanziata autorizzazione da parte dell'Area ICT.

L'utilizzo di cloud diversi da quelli interni al sistema di archiviazione di Ateneo mette a repentaglio la qualità della custodia dei dati, in quanto non esistono un'analisi preventiva e un modello di gestione integrato con il sistema di Ateneo.

Comportamenti non consentiti

Sono vietati a tutti gli utenti i seguenti comportamenti:

- l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo della smart card di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche di Unige e/o lo scambio di comunicazioni mediante falsa identità;
- l'installazione, sui dispositivi aziendali in dotazione, di software non coperto da licenza o, comunque, non autorizzato dall'Area ICT, o contrario ai regolamenti e alle leggi;
- l'abuso per motivi personali delle risorse informatiche dell'Ateneo;
- l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata o contraria ai regolamenti di file e di ogni altra risorsa informatica;
- l'allontanamento dai dispositivi senza il loro blocco o l'adozione delle opportune misure di sicurezza;
- la modifica delle configurazioni delle risorse informatiche di Ateneo senza l'autorizzazione dell'Area ICT;
- l'utilizzo di strumenti volti a eludere i sistemi di protezione.

Protezione contro furti e danneggiamenti

Tutti i dispositivi aziendali, soprattutto se mobili, devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in essi contenuti. L'Utente è tenuto a informare immediatamente il dirigente responsabile, l'Area ICT e, qualora vi sia la possibilità di una violazione di dati personali, altresì il DPO di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

Comportamento in caso di assenza programmata

Il personale dell'Area ICT, salvo per previste motivazioni di sicurezza, tecniche, o legali, non accede ai dati e ai profili dell'utente assente senza il suo consenso, né autorizza terzi all'accesso.

Pertanto, in caso di assenza programmata, al fine di garantire la continuità di servizio, all'utente è richiesto di rendere disponibili i documenti su cui sta lavorando all'ufficio di riferimento, tramite l'utilizzo delle risorse di archiviazione condivisa di Ateneo. Potrà essere utile attivare i meccanismi di risposta automatica, disponibili nelle applicazioni e dispositivi aziendali (risposte automatiche di Outlook e Teams, segreterie telefoniche) per permettere il corretto instradamento dell'attività ai colleghi.

AMBITI DI RICERCA E DIDATTICA

Le attività di ricerca e di didattica si svolgono all'interno dei regolamenti di Ateneo e delle leggi in vigore. Valgono in generale tutte regole e le raccomandazioni contenute nel presente documento e nell'insieme delle regole di Ateneo.

Le attività di ricerca e didattica si svolgono per loro natura con un elevato grado di autonomia degli utenti coinvolti e possono richiedere una maggiore varietà di configurazioni di dispositivi e di applicativi rispetto a quelli normalmente disponibili per le attività di ufficio. L'utilizzo di configurazioni, applicazioni, modalità di utilizzo diverse da quelle già considerate consone per l'attività in Ateneo richiede una consultazione preventiva del personale dell'Area ICT, secondo i normali canali di assistenza, per l'individuazione della maniera più consona di soddisfacimento della necessità (Es. una ricerca sui virus informatici potrebbe richiedere il corretto isolamento dell'ambiente di test e l'esclusione dell'accesso alla rete di produzione).

L'accesso a dati del sistema informativo di Unige, soprattutto se contenenti dati personali, l'utilizzo di applicazioni con uscita o condivisione di dati dal sistema informativo di Unige, l'iscrizione degli Utenti Unige a servizi non gestiti internamente, sono tutti esempi di attività che necessitano di consultazione preventiva dell'Area ICT.

L'Area ICT si fa carico di esaminare le necessità e cercare soluzioni che preservino in primo luogo la sicurezza dell'utente e la funzionalità dell'infrastruttura informatica di Ateneo. I casi più comuni possono essere coperti dall'osservanza di semplici indicazioni sul sito di Ateneo e più specificatamente dell'Area ICT.

La consultazione, se invece necessaria, deve avere luogo nella fase precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni, o anche procedure legali ove necessario.

CONTROLLO E MONITORAGGIO

L'Area ICT imposta la propria azione di monitoraggio e controllo sui sistemi informatici di Ateneo messi a disposizione per lo svolgimento delle attività nel rispetto della normativa vigente e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti.

A tal fine, l'Area ICT utilizza sistemi automatizzati per il monitoraggio centralizzato che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici di Ateneo e delle informazioni ivi contenute.

I file di log relativi all'utilizzo della infrastruttura informatica sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente e alle disposizioni adottate al riguardo dall'Area ICT. Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log file e i dati di monitoraggio relativi possono essere esaminati dagli amministratori di sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali. In ogni caso, tutti i controlli di funzionalità e monitoraggio avvengono nel rispetto di quanto previsto dal CAD, dalle norme in materia di tutela della libertà e dignità dei lavoratori, della normativa unionale e nazionale in materia di protezione dei dati personali.

Gli amministratori di sistema, nel caso in cui rilevino anomalie o configurazioni non corrette dei dispositivi, possono provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi di Unige. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento da parte degli amministratori di sistema. Le predette attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

RUOLI E RIFERIMENTI

Organizzazione e referenti

L'Area ICT si articola internamente in servizi e settori in modo da potere rispondere adeguatamente alle necessità informatiche dell'Ateneo.

Nell'ambito della propria attività si avvale della collaborazione di referenti qualificati individuati nelle strutture interne all'Ateneo e/o dipendenti di aziende e/o professionisti esterni a Unige, a cui l'Area ICT può delegare ruoli amministrativi e di riferimento. Nell'ambito di questo rapporto, tali figure comunque agiscono e rispondono delle proprie azioni come afferenti all'Area ICT.

Ruolo degli amministratori

Gli Amministratori dell'Area ICT svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite dall'Ateneo e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali. Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri Utenti, gli Amministratori sono tenuti ad avvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.

ASSISTENZA, INFORMAZIONE, FORMAZIONE

Gli utenti possono ottenere assistenza e informazioni tramite i canali previsti dall'Ateneo per le varie casistiche, così come pubblicato sulle pagine dell'Ateneo e più specificatamente dell'Area ICT. I canali preferenziali da cui partire con una richiesta di assistenza o di informazioni, salvo per casi specifici e diversamente indicati, sono l'Help Desk dell'Area ICT e i tecnici locali di riferimento (tecnici di dipartimento, presidii). La richiesta di assistenza o di informazioni verrà instradata internamente nella maniera più consona, al fine di fornire una risposta adeguata nel minor tempo possibile e un corretto trattamento del caso.

Gli utenti non devono cercare di contattare direttamente un supporto specialistico interno all'Area ICT, se non specificatamente indicato dal personale di supporto, né possono scegliere di essere assistiti da specifiche persone.

L'assistenza informatica dell'Ateneo copre le risorse e gli strumenti informatici di Unige, ma non quelle esterne ad esso, o comunque fuori dalla propria gestione. Esempio: può essere offerta assistenza per la configurazione della posta elettronica di ateneo, ma non per l'allestimento del computer di proprietà dell'utente. Il limite dell'intervento viene di volta in volta definito e chiarito dal personale di supporto tecnico di Unige.

Supporto all'acquisizione di risorse informatiche

L'Area ICT fornisce supporto all'acquisizione di risorse informatiche a diversi livelli, a seconda della destinazione e della finalità dell'oggetto e del successivo modello di gestione. Il livello di coinvolgimento dell'Area ICT può variare a seconda delle necessità e prevede che l'acquisto venga indirizzato per soddisfare sia le necessità tecniche immediate, sia quelle di gestione successiva. Di particolare rilevanza, nel caso dell'hardware, è la progettazione del successivo ciclo di gestione dell'oggetto. Nel caso del software, l'Area ICT si premura soprattutto di

assicurare l'individuazione del corretto applicativo, l'inserimento del software nel modello di gestione, la compatibilità con le risorse informatiche di Ateneo, la sicurezza.

La consultazione, quando necessaria, deve avere luogo nella fase di analisi del bisogno, precedente alla presa di accordi con terzi o di indagine economica. Il parere dell'Area ICT in merito è vincolante. L'Area ICT si riserva di intervenire in modo proattivo o reattivo, come necessario, in caso di inosservanza delle regole e delle raccomandazioni, pericolo per la sicurezza, o comunque quando ritenga sia necessario intervenire secondo il suo mandato. Possibili interventi sull'utente o sull'ufficio possono includere il richiamo, il blocco dell'accesso o delle autorizzazioni.

Tutte le acquisizioni di risorse informatiche dell'amministrazione centrale richiedono il coinvolgimento dell'Area ICT dal primo momento (es. uffici, stampanti, telefonia, reti, software).

Tutte le acquisizioni di risorse informatiche rivolte al pubblico o agli studenti richiedono il coinvolgimento dell'Area ICT dal primo momento (es. aule informatiche, sale conferenze, sia hardware che software).

Tutte le acquisizioni di risorse informatiche che prevedano un coinvolgimento dell'Area ICT nella gestione richiedono il coinvolgimento dell'Area ICT dal primo momento (es. dipartimenti carenti di personale tecnico informatico e assistiti dall'Area ICT, software da integrare con le risorse informatiche di Ateneo o con l'infrastruttura di autenticazione).

Per le acquisizioni di particolari tipi di apparecchiature o software le Strutture Fondamentali possono avvalersi della consulenza dell'Area ICT (es. Workstation particolarmente potenti, infrastrutture hardware e software complesse e necessitanti integrazione)

Per i dispositivi ad uso personale più comuni, si consiglia comunque una consultazione del personale tecnico locale (es. portatile personale pagato su fondi di ateneo, non per acquisti privati).

Gli acquisti di dispositivi personali da parte degli studenti non prevedono un'assistenza specifica dell'Area ICT, ma l'eventuale stipula di convenzioni richiede il coinvolgimento dell'Area ICT dal primo momento (es. sconti da particolari fornitori).

Formazione

L'Utente ha diritto ad essere formato all'utilizzo delle risorse informatiche in uso in Ateneo. L'Area ICT provvede a questo fabbisogno tramite la progettazione di corsi erogati con risorse interne ed esterne all'Ateneo. Periodicamente provvede all'erogazione di corsi ai nuovi utenti e aggiornamenti per gli utenti già presenti. In alcuni casi, l'Area ICT può richiedere l'erogazione di corsi fuori dalla pianificazione, per motivata urgenza, e corsi obbligatori per categorie di utenti, per necessità di sicurezza o di funzionamento.