UNIVERSITÀ DELLA VALLE D'AOSTA
UNIVERSITÉ DE LA VALLÉE D'AOSTE

Emanato con Decreto Rettorale n. 92 Prot. n. 12067 del 04/08/2021

REGOLAMENTO PER L'USO DELLE RISORSE INFORMATICHE DI ATENEO

Versione 3.0 giugno 2021

SOMMARIO

CAPO I. PREMESSE

ART 1. FINALITÀ E SCOPO DEL DOCUMENTO

Negli ultimi anni le attività di didattica, di ricerca, di terza missione nonché le collegate attività amministrative sono state sottoposte ad un imponente processo di informatizzazione e digitalizzazione e, in tale contesto, i servizi di rete, dai software gestionali alla posta elettronica, sono diventati strumenti quotidiani indispensabili per l'esercizio delle attività istituzionali dell'Università della Valle d'Aosta - Université de la Vallée d'Aoste (di seguito Ateneo).

Tuttavia, un uso non corretto di tali strumenti, anche a seguito di comportamenti inconsapevoli, può essere causa di gravi minacce e problemi per la sicurezza del sistema e delle informazioni in esso contenute.

Inoltre, dato che le informazioni trattate nell'ambito dell'attività lavorativa possono riguardare la sfera personale degli utenti, il trattamento dei dati e le attività di monitoraggio cui possono essere sottoposte le risorse informatiche, dovranno sempre ispirarsi al rispetto della normativa in materia di tutela della riservatezza dei dati personali nonché ai principi di diligenza e correttezza.

Il presente regolamento ha lo scopo di:

- dettare le procedure per un corretto utilizzo delle risorse informatiche messe a disposizione ai propri utenti dall'Ateneo nel rispetto della normativa vigente;
- definire il diritto dell'Ateneo di verificare il corretto utilizzo delle risorse informatiche tenendo conto della normativa con particolare riguardo alla protezione dei dati personali. Il presente regolamento costituisce, infatti, preventiva informazione delle attività di controllo nei confronti degli utenti.

ART 1. AMBITO DI APPLICAZIONE E PRINCIPI DI BUON UTILIZZO DELLE RISORSE INFORMATICHE

Il presente Regolamento si applica a tutti gli utenti che a diverso titolo accedono alle risorse informatiche dell'Ateneo.

Le risorse informatiche fornite dall'Ateneo devono essere utilizzate nel rispetto delle comuni regole in materia di sicurezza dei sistemi informatici e di tutela dei dati personali.

Gli utenti sono responsabili dell'utilizzo, anche da parte di terzi, delle risorse informatiche a loro assegnate: è necessario custodire le dotazioni in modo appropriato e diligente e utilizzarle esclusivamente per le finalità proprie dell'Ateneo: per le attività di didattica, di ricerca, di terza missione nonché per le collegate attività amministrative.

ART 2. CONTESTO NORMATIVO

I principali riferimenti normativi in materia sono i seguenti:

a) Codice dell'Amministrazione Digitale (CAD);
b) Decreto legislativo 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali";
c) Regolamento generale per la protezione dei dati personali (General Data Protection Regulation o GDPR) n. 2016/679;
d) Decreto legislativo 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)";
e) Provvedimento generale del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (27 novembre 2008 come modificato in base al provvedimento del 25 giugno 2009);
f) Linee guida del Garante per posta elettronica e internet (G.U. n. 58/2007);
g) Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di Sicurezza ICT per le pubbliche amministrazioni;
h) Regolamento interno in materia di protezione dei dati personali, emanato con decreto rettorale n. 52 del 5 giugno 2019, in attuazione del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio e del Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali.
i) Codice di comportamento dell'Ateneo;
j) Codice etico di Ateneo.

ART 3. DEFINIZIONI

Al fine dell'applicazione del presente Regolamento deve intendersi:

a) Risorsa informatica: qualsiasi tipo di hardware, computer, mezzo di comunicazione elettronica, rete di trasmissione dati, modem, stampante, scanner, apparecchiatura per l'archiviazione elettronica dei dati e relativi supporti di memorizzazione, videoterminale, software operativo e programma applicativo, dato e informazione in formato elettronico, di proprietà o comunque nella disponibilità dell'ente o ad esso concesso in licenza d'uso, ivi inclusi i servizi cloud.
b) Sistema informativo di Ateneo (SIA): l'insieme delle risorse informatiche dell'Università della Valle d'Aosta.
c) Utente: qualsiasi soggetto utilizzatore, fruitore, esecutore e gestore delle risorse informatiche. A titolo di esempio: personale docente, ricercatori, studenti, laureati, personale tecnico amministrativo, collaboratori, componenti degli organi, consulenti, cittadini.
d) Account: insieme dei dati identificativi di un utente; funzionalità, strumenti e contenuti attribuiti ad un utente in determinati contesti operativi (siti web, applicativi o software gestionali).
e) Titolare del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
f) Soggetto autorizzato al trattamento con delega (SATD): la persona fisica che tratta dati personali per conto del titolare del trattamento (rif. Art. 2-quaterdecies par. 1 del Dlgs 196 /2003);
g) Soggetto autorizzato al trattamento (SAT): la persona fisica che tratta dati personali per conto del titolare del trattamento su nomina del Soggetto autorizzato al trattamento con delega (rif. Art. 2-quaterdecies par. 2 del Dlgs 196 /2003);
h) Amministratore di sistema: persona fisica che si occupa della gestione e della manutenzione delle risorse informatiche;
i) Responsabile della sicurezza informatica: persona fisica che ha il compito di garantire la sicurezza delle infrastrutture informatiche (PC, server, apparati di rete...) e la sicurezza nella gestione degli accessi a risorse informatiche on-premise (in locale) o in cloud.

ART 4. PREMESSA METODOLOGICA

Il regolamento in oggetto deve garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Al seguente testo "statico" che contiene gli articoli che formano la base normativa del regolamento, si affiancano, quindi, una serie di misure tecniche i cui contenuti più flessibili potranno adeguarsi agevolmente all'evoluzione tecnologica.

Tali misure tecniche di dettaglio, redatte dall'Ufficio Sistemi Informatici e Statistica, sono approvate dal Direttore Generale a cui sono attribuite la complessiva organizzazione e gestione dei servizi, delle risorse strumentali e del personale tecnico-amministrativo dell'Ateneo.

CAPO II. SISTEMA INFORMATIVO DI ATENEO

ART 5. SISTEMA INFORMATIVO QUALE INSIEME DELLE RISORSE INFORMATICHE DI ATENEO

L'insieme delle risorse informatiche di cui l'Ateneo dispone per il trattamento delle informazioni e dei dati come hardware (personal computer, notebook, server, stampanti, fotocopiatrici e periferiche varie), software (programmi informatici di base e applicativi, gestionali, database, ecc.) e reti telematiche, nonché le informazioni e i dati stessi formano il Sistema Informativo di Ateneo (da ora denominato SIA).

Le risorse informatiche che l'Ateneo mette a disposizione degli utenti per lo svolgimento del proprio lavoro sono di esclusiva proprietà dello stesso e devono essere utilizzate unicamente per gli scopi dell'Ateneo. È quindi vietato l'utilizzo delle risorse informatiche per scopi personali.

L'Ateneo si riserva la facoltà di ricorrere contro comportamenti da parte degli utenti in contrasto con le leggi vigenti e/o il presente Regolamento.

ART 6. CONFORMITÀ AL GDPR E AL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI E AI REGOLAMENTI INTERNI

Il SIA gestisce dati personali così come definiti dal Regolamento generale per la protezione dei dati personali (General Data Protection Regulation o GDPR) n. 2016/679.

L'Ateneo, in qualità di Titolare del Trattamento di Dati Personali, è tenuto a tutti gli adempimenti di legge in materia di protezione dei dati personali.

È stato adottato il Regolamento interno in materia di protezione dei dati personali, con decreto rettorale n. 52 del 5 giugno 2019, in attuazione del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio e del Decreto Legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali.

La designazione a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 è da intendere rivolta a soggetti esterni alla struttura del Titolare.

L'equivalente funzione, per utenti alle dipendenze dell'Ateneo, viene assegnata a Soggetti Autorizzati al Trattamento di dati personali con Delega (SATD), ai sensi dell'art. 2-quaterdecies del D. Lgs. 196/2003, così come novellato dal D. Lgs. 101/2018 (Codice in materia di protezione dei dati personali).

I Soggetti Autorizzati al Trattamento di dati personali con Delega (SATD) sono così individuati:

a) per le attività di competenza del Rettorato: il Rettore o un suo delegato espressamente designato;
b) per le strutture amministrative e gestionali: il Direttore Generale per le attività di competenza della direzione generale e i dirigenti di Area per le rispettive attività di competenza;
c) per le attività di didattica e di ricerca: i direttori dei dipartimenti e dei centri di ricerca, i responsabili dei progetti di ricerca.

I SATD nominano i Soggetti Autorizzati al Trattamento dei dati (SAT - ex Incaricati al Trattamento dei Dati), ai sensi dell'art. 2-quaterdecies comma 2 del Codice in materia di protezione dei dati personali, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione.

I SATD nominano gli Amministratori di sistema autorizzandoli alla gestione e alla manutenzione le risorse informatiche dell'Ateneo (SIA).

I SATD adottano idonei sistemi di registrazione degli accessi logici alle risorse informatiche da parte degli Amministratori di sistema. Tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Inoltre, devono comprendere riferimenti temporali, la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

ART 7. MISURE GENERALI DI SICUREZZA

Le componenti del SIA (hardware, software, reti) sono gestite e manutenute dal personale nominato "Amministratore di sistema" o da soggetti (personale dell'Ateneo, imprese, consulenti, ecc.) che operano su incarico e per conto degli stessi. Nessun altro soggetto è autorizzato ad operare sul SIA.

Qualunque soggetto esterno incaricato della manutenzione e gestione del SIA, dovrà sempre essere identificabile per mezzo di appositi segni distintivi che ne certifichino l'autorizzazione ad agire. In caso di dubbio o sospetto, sarà compito di ogni Utente segnalare all'Amministratore di sistema la potenziale anomalia.

Qualsiasi richiesta di intervento tecnico di qualsiasi natura sul SIA deve essere gestita e autorizzata dall'Amministratore di sistema. Non è permesso intervenire autonomamente o ricorrere in modo autonomo a prestazioni tecniche fornite da soggetti esterni.

Ogni utente del SIA è tenuto ad osservare i comportamenti previsti dal presente Regolamento e dalle relative misure tecniche di dettaglio per garantire la massima sicurezza delle informazioni e l'integrità funzionale degli strumenti utilizzati.

È compito di ogni utente segnalare all'Amministratore di sistema situazioni di utilizzo non autorizzato o contrario alla legge degli strumenti informatici, eventuali casi di difficile interpretazione nonché qualsiasi malfunzionamento degli strumenti informatici in uso.

ART 8. ACCESSO AL SISTEMA INFORMATIVO DI ATENEO

L'accesso al SIA è consentito unicamente agli utenti aventi un account fornito dall'Ateneo, quindi in possesso di credenziali di autenticazione rilasciate dallo stesso tramite apposite procedure informatiche. Alcuni servizi definiti dall'Amministratore di sistema potranno essere aperti all'uso tramite credenziali pubbliche, emesse da enti con cui l'Ateneo ha stipulato convenzioni specifiche.

Le credenziali di autenticazione sono strettamente personali e devono essere utilizzate, esclusivamente, dall'utente titolare che provvederà a custodire e a garantire la segretezza della parola chiave e a modificarla, con cadenza almeno trimestrale, secondo le politiche di Ateneo.

L'identificativo utente deve essere inserito all'avvio della sessione di lavoro e permette al SIA di riconoscere l'utente e di consentire l'accesso alle risorse informatiche per le quali è autorizzato (archivi, servizi, internet, posta elettronica, wifi, ecc.).

L'Amministratore di sistema è responsabile della gestione delle credenziali di autenticazione degli utenti emesse direttamente dall'Ateneo. Per le credenziali ottenute da soggetti terzi ma autorizzate all'accesso al SIA, l'utente è responsabile della conservazione, gestione e rinnovo presso il soggetto terzo.

Ai SATD compete la richiesta di nuova credenziale e di revoca di credenziale esistente. Le richieste di rilascio o di revoca di credenziali di autenticazione devono essere inoltrate in forma scritta all'Amministratore di sistema anche via mail. Nella richiesta il SATD dovrà precisare a quali risorse informatiche l'utente dovrà essere abilitato, come ad esempio archivi (database), programmi, cartelle, internet, posta elettronica, ecc. Non saranno prese in considerazione richieste di credenziali di autenticazione formulate da soggetti diversi dai SATD. La revoca potrà essere inoltre eseguita d'ufficio dall'Amministratore di sistema, manualmente o per mezzo di sistemi automatizzati, in tutti i casi che prevedano la perdita dei requisiti di Utente del SIA.

ART 9. UTILIZZO DELL'HARDWARE

La Direzione Generale dell'Ateneo, tramite i competenti uffici, provvede all'acquisto delle risorse informatiche. La tipologia, la dotazione e la configurazione delle apparecchiature informatiche e delle postazioni di lavoro sono definite sulla base delle esigenze degli utenti e della necessaria integrazione e compatibilità con il SIA.

La configurazione delle apparecchiature informatiche dell'Ateneo è realizzata su modelli valutati dall'Amministratore di sistema, al fine di garantire la semplicità di gestione del parco macchine e la condivisione delle risorse informatiche tra tutti gli utenti del SIA. Di conseguenza non è permesso modificare la configurazione hardware delle dotazioni in assegnazione. In particolare, non è permesso spostare i seguenti dispositivi dagli uffici e dalle aule: monitor o stampanti, fotocopiatrici, scanner, telefoni, e installare o disinstallare dispositivi hardware (banchi di memoria, schede, mouse, stampanti, ecc.) dai pc o notebook in dotazione, se non a seguito di autorizzazione dell'Amministratore di sistema.

L'installazione, configurazione e manutenzione di tutte le componenti del SIA compete al personale di Ateneo in proprio o attraverso l'ausilio di personale esterno a tale scopo incaricato.

È vietata la cessione ai terzi degli apparati assegnati dall'Ateneo.

Il presente regolamento si applica anche ai dispositivi mobili quali notebook, smartphone e qualsiasi ulteriore accessorio hardware eventualmente assegnati dall'Ateneo agli utenti e da questi utilizzati anche al di fuori della rete locale e degli uffici dell'Università della Valle d'Aosta.

ART 10. UTILIZZO DEL SOFTWARE

La Direzione Generale dell'Ateneo, tramite i competenti uffici, provvede all'acquisto delle licenze d'uso dei pacchetti applicativi necessari all'informatizzazione dell'Ateneo. Le caratteristiche del software applicativo acquistato sono definite sulla base delle esigenze degli utenti e della necessaria integrazione e compatibilità con il SIA.

Le licenze d'uso dei pacchetti applicativi acquisiti dalla Direzione Generale sono di proprietà dell'Ateneo.

I programmi applicativi sviluppati in proprio dall'Ateneo attraverso i propri dipendenti o da terzi appositamente incaricati, al fine di soddisfare esigenze di informatizzazione delle attività degli utenti dell'Università della Valle d'Aosta, sono di proprietà esclusiva dell'Ateneo medesimo.

L'utilizzo di tutti i programmi applicativi installati sulle postazioni di proprietà dell'Ateneo è limitato ai casi e agli scopi previsti dall'Ateneo.

Per prevenire l'introduzione di programmi dannosi e proteggere l'integrità del SIA e garantire la compatibilità funzionale, tecnica e il mantenimento dell'efficienza operativa del SIA i nuovi software devono essere installati solo dopo parere positivo degli Amministratori di sistema. A tal fine l'interessato deve formulare richiesta scritta, anche via mail, almeno una settimana prima del necessario in modo che gli Amministratori di sistema possano procedere con le dovute prove di funzionamento e di compatibilità.

A conclusione di ogni sessione di lavoro o per interruzioni di durata significativa, l'utente è tenuto a chiudere l'applicazione in uso, seguendo le procedure previste (disconnessione dell'utente).

L'utente è tenuto ad impostare ed attivare il blocco schermo con password del sistema operativo in caso di allontanamento, anche temporaneo, dalla postazione di lavoro, al fine di evitare di lasciare la risorsa informatica incustodita.

Al fine di garantire la salvaguardia e la sicurezza delle risorse informatiche, gli amministratori di sistema, nell'ambito delle funzioni manutentive di pertinenza, potranno effettuare attività di verifica e nel caso procedere alla rimozione di ogni file e/o software potenzialmente pericolosi.

Costituiscono buone regole cancellare i file inutili ed evitare l'archiviazione ridondante che non consenta in modo chiaro l'identificazione dello stato di revisione del documento.

È vietata la duplicazione o copia parziale del software installato nel SIA, con esclusione delle copie di salvataggio effettuate dall'Amministratore di sistema.

L'utente deve segnalare qualsiasi malfunzionamento o errore dei programmi applicativi in uso all'Amministratore di sistema nei tempi più brevi; la segnalazione deve essere chiara e completa e, se possibile, deve evidenziare le condizioni in cui si è verificato l'errore.

Non è permesso modificare la configurazione software dei computer. In particolare, sono tassativamente vietate l'alterazione dei parametri di configurazione del sistema operativo.

Gli utenti che in seguito alla volontaria manomissione della propria postazione di lavoro provocheranno la perdita di dati o comunque malfunzionamenti delle apparecchiature, saranno ritenuti responsabili degli eventuali danni arrecati all'Ateneo.

ART 11. UTILIZZO DELLA RETE DATI DI ATENEO E DELLA RETE WIFI

È vietato il collegamento alla rete locale di Ateneo di apparecchiature non di proprietà dell'Università, salvo specifica autorizzazione dell'Amministratore di sistema.

È disponibile, per gli utenti dell'Università, l'accesso al servizio Internet tramite rete WIFI di Ateneo. L'accesso WIFI è consentito anche con apparecchiature personali, fermo restando il rispetto delle norme sull'utilizzo di Internet del presente regolamento.

ART 12. UTILIZZO DI INTERNET

L'Ateneo mette a disposizione nelle proprie sedi e ai propri utenti abilitati il servizio di navigazione Internet.

Gli utenti devono utilizzare il collegamento ad Internet per motivi istituzionali e sono considerati responsabili delle attività espletate in rete mediante le credenziali di accesso e di autorizzazione individuali.

È vietato il download (memorizzazione sul disco del proprio computer o su altri dispositivi di memorizzazione, anche rimovibili) di file o archivi di qualsiasi genere trovati durante la navigazione su Internet, se non per motivi strettamente legati alla propria attività. In particolare, è vietato il download di contenuti protetti dalle leggi sul diritto d'autore (software, brani musicali, films, fotografie, ecc.).

Nel caso di scarico autorizzato di file da Internet, gli stessi devono essere immediatamente verificati con il software antivirus.

L'Ateneo, in rete locale, adotta sistemi automatici di filtraggio degli indirizzi Internet (URL filtering) per impedire l'accesso da parte degli utenti a siti vietati. Le modalità di filtraggio degli indirizzi Internet sono diversificate in base alle esigenze ed alle attività degli uffici, aree o progetti di ricerca. Tali esigenze sono segnalate per iscritto dai SATD interessati all'Amministratore di sistema anche via mail.

L'Ateneo può avvalersi dei medesimi sistemi di cui al punto precedente anche ai fini di documentare il traffico internet generato dalle postazioni della rete locale. Tali informazioni sono raccolte unicamente allo scopo di verificare ex-post utilizzi illeciti del collegamento ad Internet che abbiano causato danni all'Ateneo, o per controlli difensivi, oppure nell'ambito di indagini condotte dall'Autorità Giudiziaria. La raccolta e la custodia delle informazioni di navigazione sono effettuate nelle modalità previste dalla normativa vigente. La garanzia e tutela delle informazioni trattate saranno assicurate in osservanza delle disposizioni di Legge in materia di Privacy e degli atti emanati dal Garante.

ART 13. UTILIZZO DELLA POSTA ELETTRONICA

L'Ateneo mette a disposizione dei propri utenti abilitati l'utilizzo del servizio di posta elettronica.

Sono utenti abilitati gli appartenenti ai seguenti gruppi: personale docente di ruolo o a contratto, personale amministrativo a tempo indeterminato o determinato e studenti.

Su richiesta del SATD dell'area, della struttura o del dipartimento di riferimento possono essere abilitati ricercatori, assegnisti, cultori della materia o altri collaboratori.

Non è permesso l'utilizzo delle caselle di posta fornite dall'Ateneo per motivi privati non inerenti alle attività istituzionali aventi ad oggetto dati personali ex Dlgs n. 196/2003 e Reg. UE n. 679/2016 e s.m.e i.

L'utenza di posta elettronica è strettamente personale. L'utente si assume ogni responsabilità per un utilizzo improprio.

L'utente non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato, messaggi che contengano o rimandino a:

a) pubblicità non istituzionale, manifesta o occulta;
b) comunicazioni commerciali private;
c) comunicazioni di propaganda politica esterna all'Ateneo;
d) materiale pornografico o similare;
e) materiale discriminante o lesivo in relazione a razza, sesso, religione, orientamento politico, ecc.;
f) materiale che violi la normativa sulla privacy;
g) contenuti o materiali che violino i diritti di proprietà di terzi;
h) contenuti diffamatori o palesemente offensivi;
i) altri contenuti illegali.

Le caselle di posta elettronica sono di esclusiva proprietà dell'Ateneo.

Le caselle possono essere intestate a uffici e/o gruppi. A queste potranno accedervi singoli utenti o gruppi di utenti a seconda delle esigenze organizzative. In caso di accesso consentito a gruppi di utenti le credenziali per ciascun componente del gruppo saranno le stesse di quelle del singolo.

I titolari di una casella di posta elettronica con un indirizzo riportante il proprio nominativo (es: m.rossi@univda.it) sono tenuti ad indicare in calce alle proprie e-mail un avvertimento ai destinatari nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente come indicato al punto 5.2, lettera b), ultimo capoverso delle Linee guida del Garante per posta elettronica e internet (G.U. n. 58/2007), secondo le seguenti specifiche:

Nome Cognome

Ufficio / Ruolo

Università della Valle d'Aosta - Université de la Vallée d'Aoste

Indirizzo

Telefono

Mail

Questo messaggio e i suoi allegati sono indirizzati esclusivamente alle persone indicate. La diffusione, copia o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate. Eventuali risposte a questo messaggio potranno essere conosciute nell'organizzazione di appartenenza del mittente,

secondo quanto previsto dal Regolamento per l'uso delle risorse informatiche di Ateneo. Qualora abbiate ricevuto questo documento per errore siete cortesemente pregati di dame immediata comunicazione al mittente e di provvedere alla sua distruzione. Grazie.

In caso di assenza prolungata dell'utente titolare, il SATD potrà provvedere ad assegnare la delega alla consultazione della casella ad altro utente, avvertendo senza indugio l'utente titolare.

L'Amministratore di sistema adotta le misure di sicurezza necessarie a minimizzare il rischio di interruzione del servizio di posta e/o di perdita di informazioni. Si avvale, a tal fine, di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi di posta che potrebbero compromettere il servizio. In queste attività di controllo l'Amministratore di sistema potrebbe venire a conoscenza di informazioni contenute nelle mail personali degli utenti.

ART 14. PROTEZIONE ANTIVIRUS

Ogni utente è tenuto a adottare comportamenti tali da ridurre il rischio di attacco da parte di virus o di ogni altro software che operi con lo scopo di superare le difese di sicurezza del Sistema Informativo di Ateneo (SIA).

Il software antivirus installato sulle dotazioni di Ateneo è aggiornato in modo automatico secondo le procedure definite dall'Amministratore di sistema.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) segnalare l'accaduto all'Amministratore di sistema.

Non è consentito l'utilizzo di dispositivi amovibili (CD/DVD, USB pen drive e simili) personali o comunque non forniti dall'Ateneo.

Si consiglia di evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile. Si consiglia inoltre di non aprire file allegati a e-mail provenienti da utenti sconosciuti.

ART 15. GESTIONE DEGLI ARCHIVI INFORMATICI (LOCALI O IN CLOUD)

È buona prassi che le informazioni prodotte dagli utenti (documenti, archivi, dati in generale), non siano memorizzate in locale sui PC ma siano memorizzate unicamente su cartelle predisposte sui dispositivi di rete appositamente configurati dall'Amministratore di sistema. Ciascun utente potrà accedere solamente ai dati contenuti all'interno della cartella (e sottocartelle) dell'ufficio, area o progetto di ricerca di appartenenza, salvo eccezioni dettate da esigenze organizzative. Scopo di queste cartelle è la creazione dell'archivio delle informazioni prodotte dagli utenti, nonché la condivisione delle informazioni tra gli utenti dello stesso ufficio, area o progetto di ricerca.

L'Amministratore di sistema espleterà le attività volte a garantire la sicurezza delle informazioni memorizzate sulle cartelle di rete attraverso periodiche copie di salvataggio degli archivi.

I singoli utenti sono comunque responsabili della integrità, della disponibilità e della riservatezza delle informazioni memorizzate nelle cartelle alle quali hanno accesso.

Non è consentita la copia di archivi contenenti dati dell'Ateneo di qualsiasi genere o specie su dispositivi amovibili (CD/DVD, USB pen drive e simili) né su dispositivi di memorizzazione esterni all'Ateneo diversi da quelli specificamente autorizzati dall'Ateneo e per i quali è prevista la crittografia dei dati. È quindi vietato effettuare inutili duplicazioni di dati su dispositivi amovibili.

Gli Amministratori di sistema, nell'ambito delle attività di gestione e manutenzione del parco macchine, effettuano controlli periodici sui PC in uso agli utenti e sui dispositivi di memorizzazione. Gli archivi, i programmi installati e le modifiche alla configurazione dei PC, non precedentemente autorizzati, saranno cancellati previa segnalazione al SATD di competenza, il quale provvederà a porre in atto eventuali provvedimenti disciplinari.

ART 16. UTILIZZO DELLA FIRMA DIGITALE

L'Ateneo assegna agli utenti autorizzati un certificato di firma digitale per la sottoscrizione di documenti informatici nell'ambito delle attività istituzionali, tramite il personale incaricato del riconoscimento. Il personale incaricato del servizio di firma digitale, dell'identificazione, dell'attivazione, sospensione e revoca dei certificati è nominato dal SATD.

I SATD delle diverse aree o strutture di ricerca, con comunicazione al personale incaricato del riconoscimento, anche via mail, individuano gli utenti assegnatari del certificato di firma digitale.

Gli assegnatari, nel rispetto dei poteri di firma derivanti dalla legge e dalle disposizioni di cui ai regolamenti e alle procedure di Ateneo, adottano tutte le misure organizzative e tecniche idonee all'utilizzo personale della firma per

evitare l'uso fraudolento da parte di terzi. Gli assegnatari informano gli incaricati del riconoscimento di ogni circostanza che renda necessaria o, comunque, opportuna la sospensione o la revoca del certificato di firma.

ART 17. UTILIZZO DEL MATERIALE DI CONSUMO

La Direzione Generale dell'Ateneo tramite i competenti uffici provvede all'acquisto di materiale di consumo (toner, carta, ecc), necessari per il funzionamento delle risorse informatiche. Le caratteristiche del materiale di consumo acquistato sono definite sulla base delle esigenze degli utenti e della necessaria integrazione e compatibilità con le apparecchiature stesse. L'utilizzo di tale materiale è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali e/o utilizzi impropri.

ART 18. UTILIZZO DELLE APPARECCHIATURE TELEFONICHE

La Direzione Generale dell'Ateneo tramite i competenti uffici provvede all'acquisto delle apparecchiature telefoniche necessarie per l'espletamento dell'attività degli utenti dell'Ateneo. La tipologia, la dotazione e la configurazione delle apparecchiature telefoniche sono definite sulla base delle esigenze degli utenti, del SATD e della integrazione e compatibilità con il SIA.

Fermo restando il rispetto dei principi e dei doveri di cui agli articoli precedenti, l'utilizzo delle utenze telefoniche di servizio per scopi personali è consentito solo in caso di urgenza, a fronte di occasionali ed improrogabili esigenze private.

Al fine di garantire un corretto utilizzo dei servizi di telefonia l'Ateneo predispone, ove tecnicamente possibile, adeguate profilazioni che consentano l'effettuazione o meno delle diverse tipologie di chiamata.

ART 19. RESPONSABILE DELLA SICUREZZA INFORMATICA

Il Consiglio dell'Università nomina il Responsabile della sicurezza informatica che ha il compito di garantire la sicurezza delle infrastrutture informatiche (PC, server, apparati di rete...) e la sicurezza nella gestione degli accessi a risorse informatiche on-premise o in cloud e ne definisce i compiti:

a) Assessment della sicurezza: valutare lo stato dell'arte della sicurezza in Ateneo e individuare un piano strategico per aumentare la capacità di reagire alle cyber minacce;
b) Definizione delle policy: definire regole e standard per la gestione della sicurezza;
c) Analisi del rischio cyber: comprendere le vulnerabilità e le minacce per l'Ateneo in modo da compiere scelte adeguate alla gestione del rischio cyber in termini di politiche e strumenti;
d) Definizione delle architetture: disegnare l'architettura per la gestione della sicurezza e monitoraggio delle scelte strutturali;
e) Identificazione delle minacce: essere aggiornati sulle tipologie di minacce e di attacco;
f) Monitoraggio della sicurezza: controllare il traffico sui diversi canali sviluppando un Security Operation Center (SOC) interno all'Ateneo o collaborando con un provider esterno;
g) Risposta agli incidenti: rispondere in tempi brevi in caso di data breach per limitarne gli effetti;
h) Investigazione forense: condurre indagini forensi in caso di data breach, collaborando con risorse interne o specialisti esterni;
i) Coordinamento gruppo sicurezza ICT.

ART 20. MONITORAGGIO E CONTROLLI

I competenti uffici della Direzione Generale dell'Università della Valle d'Aosta adotteranno ogni accorgimento tecnico necessario a tutelare l'Ateneo da eventuali comportamenti non consentiti, salvaguardando, allo stesso tempo, il rispetto della libertà e della privacy degli utenti.

I trattamenti dati relativi sono ispirati ai canoni di trasparenza e rispettano il principio di pertinenza e non eccedenza.

Il Responsabile della sicurezza effettua il monitoraggio periodico del SIA con analisi del traffico di rete, del traffico internet e inventario delle risorse hardware e software per verificare l'attuazione del presente regolamento e ridurre i possibili rischi alla sicurezza informatica.

L'Ateneo si riserva di effettuare specifici controlli sui software caricati sul personal computer o notebook assegnati agli utenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Qualora emerga un evento dannoso, una situazione di pericolo o un utilizzo non aderente al presente regolamento, il Responsabile della sicurezza segnala gli episodi al Direttore Generale che provvederà, in prima istanza, a inviare un

avviso generalizzato a tutti gli utenti dell'Ateneo ad attenersi scrupolosamente al presente regolamento. Nel caso in cui le irregolarità persistano verranno effettuati controlli su base individuale.

Nel caso di segnalazioni di attività illegittime, che hanno causato danno all'Ateneo o che ledono diritti di terzi, l'Ateneo si riserva di effettuare specifici controlli nel rispetto della normativa vigente. Peraltro, in nessun caso, ad eccezione di specifica richiesta da parte dell'Autorità Giudiziaria, verranno attuate azioni quali: la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica); la memorizzazione di quanto visualizzato sul monitor dagli utenti; la riproduzione o memorizzazione delle pagine web visualizzate dall'utente.

ART 21. SANZIONI

Gli utenti sono responsabili per qualsiasi utilizzo delle risorse informatiche dell'Ateneo non conforme alle disposizioni del presente regolamento e/o alle leggi vigenti.

L'infrazione delle presenti regole comporta l'applicazione delle disposizioni previste dal Codice Etico e dal Codice di comportamento dell'Ateneo, fermo restando l'obbligo dell'Ateneo di segnalare all'Autorità Giudiziaria eventuali violazioni a potenziale rilevanza penale.

ART 22. ABROGAZIONI

Il presente regolamento sostituisce ogni precedente regolamentazione relativamente ai temi trattati.

Il Regolamento per l'utilizzo dei laboratori multimediali emanato con Decreto Rettorale n. 61, prot. n. 2653/A3 del 7 luglio 2004 è abrogato.

ART 23. DELEGA AL DIRETTORE GENERALE

Il Consiglio dell'Università delega il Direttore Generale ad approvare le misure tecniche di dettaglio in continuo aggiornamento evolutivo elencate di seguito a titolo esemplificativo e non esaustivo:

- Provisioning utenti - gestione autenticazione – policies password, attivazione e disattivazione utenza;
- Rete wifi;
- Risorse informatiche hardware (notebook, postazioni personali, postazioni aule informatiche, postazioni aule didattiche e totem);
- Firma digitale.