UNIVERSITÀ
DEGLI STUDI
DI TORINO

Estratto
Policy di Sicurezza Informatica dell'Università degli Studi di Torino

Il presente documento è un estratto delle Policy di Sicurezza Informatica dell'Università di Torino approvate dal Consiglio di Amministrazione in data 26/05/2020. La versione integrale è disponibile sulla Intranet di Ateneo. In questo documento sono riportate le parti principali inerenti gli aspetti dei servizi online agli studenti.

Versione: 1.0
Data ultima revisione: 11-05-2020

REVISIONI

Data	Versione	Descrizione Modifica	Autore
11/05/2020	1.0	Versione Iniziale	Direzione SIPE

RIFERIMENTI

1. *Codice per l'amministrazione digitale (dlgs 82/2005);*
2. *Linee guida del Garante per posta elettronica e internet del 10 marzo 2007;*
3. *Regolamento per il trattamento dei dati sensibili e giudiziari dell'Università degli Studi di Torino ai sensi D.Lgs. 196/2003, emanato con D.R. n. 1819 del 12 marzo 2007*
4. *Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 679/2016)*
5. *Codice privacy decreto legislativo 196/2003 novellato dal D.Lgs 101/2018;*
6. *Linee guida del garante privacy per la posta elettronica ed internet, provvedimento n.13/2007*
7. *Regolamento di attuazione del Codice in materia di protezione dei dati personali dell'Università degli Studi di Torino, emanato con D.R. n. 870 del 4 marzo 2019;*
8. *Misure minime di sicurezza ICT per le pubbliche amministrazioni, da ultimo Circolare dell'Agenzia per l'Italia Digitale (Agid) n.2/2017 del 18 aprile 2017;*
9. *Legge 18 marzo 2008, numero 48 sui reati informatici;*
10. *Statuto dell'Università degli Studi di Torino, emanato con D.R. n. 1730 del 15 marzo 2012 e s.m.i.*
11. *Intranet di Ateneo, voci Sicurezza informatica e Privacy - Amministratori di Sistema*
12. *Legge 300/1970 (Statuto dei lavoratori), con riferimento in particolare all'art.4, comma 1;*
13. *D.Lgs. n. 151/2015 (cd. Job Act)*

Sommario

1. Introduzione

L'utilizzo delle risorse informatiche e telematiche deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra l'Ateneo ed i propri dipendenti e tra gli studenti e l'Ateneo con tutte le cautele necessarie per evitare le eventuali conseguenze dannose alle quali un utilizzo non corretto di tali strumenti può condurre; il tutto in considerazione anche della netta linea di confine tra l'attività lavorativa, la vita privata del lavoratore e di terzi .

La sicurezza delle informazioni è caratterizzata dai seguenti aspetti:
a) Riservatezza: garantisce che l'informazione sia accessibile solamente a coloro che hanno l'autorizzazione ad accedervi;
b) Integrità: garantisce l'accuratezza e la completezza dell'informazione e dei metodi di elaborazione;
c) Disponibilità: garantisce che gli utenti autorizzati possano accedere all'informazione quando vi è necessità.
L'utilizzo, quindi, delle risorse e dei servizi informatici dell'Ateneo deve avvenire:

- nel rispetto delle leggi e norme vigenti e in particolare delle leggi in materia di sicurezza, privacy, copyright, accesso e uso dei sistemi informatici e telematici;

- nel rispetto dei diritti alla riservatezza e alla dignità come sancito dal Regolamento sulla protezione dei dati personali (GDPR) e Regolamento Privacy di Ateneo al fine di garantire la massima efficienza delle risorse informatiche e del loro utilizzo;

- nel rispetto delle norme in materia di rapporto alle dipendenze della pubblica amministrazione, dei codici di condotta dei pubblici dipendenti e procedure lavorative generali definite dall'Ateneo~~;~~

- nel rispetto dei diritti degli altri utenti e di terzi.

La Direzione competente per i sistemi informativi, in particolare, è titolare della gestione dei sistemi informativi e promozione di politiche di sicurezza con la definizione di misure informatiche, tecnologiche e procedurali volte a sostegno della continuità operativa e alla riduzione al minimo dei rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme a dati e documenti.

Il presente documento si applica a tutti gli utenti dell'Ateneo, ovvero al Personale Docente e Tecnico Amministrativo dell'Ateneo, agli studenti e a tutti coloro che, in virtù di un rapporto di lavoro o fornitura, per esempio consulenti, collaboratori, fornitori, ecc., trattano informazioni e utilizzano sistemi informativi o apparecchiature elettroniche di proprietà dell'Università degli Studi di Torino.

Questo documento di Policy ha lo scopo di "sistematizzare" in forma struttura ed organica l'insieme delle regole tecnico-procedurali già in uso e sintesi dell'esperienza sui processi amministrativo-gestionali dell'ateneo oltre che delle norme in materia di ICT.

(OMISSIS)

2. Ruoli, organizzazione e responsabilità. Amministratori di Sistema ed Autorizzati al trattamento dei dati

L'Ateneo tratta i dati personali ai soli fini dell'erogazione e gestione dei servizi e nell'ambito delle finalità istituzionali, nel rispetto dei diritti e libertà fondamentali, nonché della dignità dell'interessato, attuando tutte le misure necessarie e sufficienti a minimizzare il rischio di perdita, distruzione o accesso abusivo d'informazioni.

Le politiche in materia di servizi ICT sono programmate e gestite dalla Direzione Sistemi Informativi, Portale, E-learning nell'ambito del Piano Operativo Portale, Sistemi Informativi e Learning (in sostanza l'agenda digitale di Unito), il processo annuale finalizzato alla raccolta e alla condivisione delle esigenze in termini di flussi informativi e di servizi del Portale Federale espresse da tutte le strutture istituzionali dell'Ateneo.

L'Ateneo nomina attraverso i Responsabili del trattamento:

1. gli **"Amministratori di Sistema**", ovvero, secondo il Provvedimento del Garante avente ad oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", persone fisiche che si occupano di gestione, di manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi di software complessi, nella misura in cui consentano di intervenire sui dati personali
2. gli **"autorizzati al trattamento**" capaci di intervenire sui dati e compiere operazioni di trattamento che, pur non essendo preposti ordinariamente a operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali.

Vanno considerati a tutti gli effetti alla stregua di trattamenti di dati personali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware, anche quando non consultati "in chiaro" dall'amministratore.

3. Identità digitale

L'accesso ai servizi telematici dell'Università di Torino che richiedono un'opportuna abilitazione alle funzionalità disponibili, presuppone il riconoscimento dell'identità del soggetto incaricato (utente) mediante il rilascio di apposite credenziali personali.

L'identità digitale degli utenti dell'Ateneo è individuabile in una delle seguenti tipologie:

- sistema pubblico per la gestione dell'identità digitale – Spid (disponibile per gli utenti che hanno ottenuto le credenziali Spid da uno degli enti autorizzati);
- sistema di credenziali unificate – SCU - per l'accesso ai servizi on line nel formato username e password (disponibile per tutte le tipologie di utenti abilitati);

(OMISSIS)

- account guest (ospiti) disponibili per soggetti esterni per i quali si renda necessario l'accesso temporaneo ai servizi

dell'Ateneo (nello specifico e per esempio il wifi e/o il sistema dei thinClient tipicamente presenti nelle aule informatiche o in alcune biblioteche o nella postazione docente delle aule per la didattica frontale);

- credenziali di autenticazione/autorizzazione di accesso a ESSE3/ESSE3PA disponibili per gli utenti incaricati di verificare le autocertificazioni presentate da studenti e laureati e di visualizzare i dati di carriera in modalità on line.

-

(OMISSIS)

- credenziali di autenticazione/autorizzazione di accesso a IRIS disponibili per gli utenti incaricati di gestire prodotti e progetti di ricerca.

(OMISSIS)

Le credenziali di autenticazione sono strettamente personali e riservate, il loro uso improprio comporta responsabilità per azioni dolose e colpose imputabili al titolare; per gli account organizzativi l'eventuale uso improprio è imputabile al Responsabile individuato in fase di richiesta/creazione dell'account stesso.

Il sistema di identità digitale (credenziali SCU) obbliga gli utenti a modificare con cadenza semestrale la password associata alla propria username SCU per l'accesso ai servizi.

Per gli "ospiti" (account guest) la scadenza è prevista in fase di accreditamento (effettuata tipicamente dal RIF di identità digitale sulla base di quanto previsto dalle linee guida per i rif) fino ad un massimo di tre mesi (con possibilità di rinnovo). Vi è una particolare categoria di guest detta long-guest la cui scadenza è fissata fino ad un massimo di 1 anno e che viene utilizzata in casi particolari (quando un utente occasionale ha una permanenza in Ateneo di massimo 1 anno ma, per esempio, non necessita di servizi particolari se non il Wifi).

(OMISSIS)

L'accesso ai servizi on line e le credenziali SCU degli studenti (username e password) restano attive non oltre il quinto anno successivo al conseguimento del titolo (al fine di favorire l'eventuale prosecuzione dei livelli superiori di corso di studio). Decorso il termine le credenziali SCU sono definitivamente disattivate, al netto di casi di prosecuzione di carriera.

I dettagli sul processo di accreditamento per l'identità digitale è qui riportato) Portale collegamento istruzioni e supporto per il login https://www.unito.it/servizi/servizi-line/istruzioni-e-supporto)

(OMISSIS)

3.1 Software d'Ateneo

È vietato, se non espressamente autorizzati dall'Ente, la duplicazione e qualsiasi forma di estensione d'uso del software aziendale, inteso sia come software prodotto direttamente dall'Ateneo sia come software prodotto da terzi ed utilizzato dall'Ateneo in forza di appositi contratti di licenza d'uso. Anche il software di Ateneo infatti è pienamente tutelato dalla normativa vigente in materia di copyright ed un suo utilizzo non autorizzato è vietato.

(OMISSIS)

4. Posta Elettronica

La casella di posta elettronica è uno strumento dell'Università di Torino finalizzato allo scambio di informazioni

(OMISSIS)

L'assegnazione di un indirizzo di posta elettronica avviene contestualmente all'assegnazione delle credenziali di autenticazione dell'Utente; di norma l'indirizzo di posta viene creato utilizzando nome.cognome e tutti gli indirizzi presentano lo stesso dominio istituzionale: @edu.unito.it. I casi di omonimia sono gestiti distintamente.

L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante credenziali di autenticazione (nome utente e password). Gli utenti assegnatari delle caselle di posta elettronica sono i diretti responsabili del corretto utilizzo delle stesse e rispondono personalmente dei contenuti trasmessi. In particolare l'Utente è tenuto a rispettare quanto segue:

- non utilizzare il servizio per scopi illegali o in maniera tale da recare danno o pregiudizio all'Ateneo o a terzi;

- non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti.

- non utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino ad esempio a: pubblicità non istituzionale, manifesta o occulta; prodotti di natura politica; comunicazioni commerciali private; materiale pornografico o simile; materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.; materiale che violi la privacy; contenuti o materiali che violino i diritti di proprietà di terzi; altri contenuti illegali.

In nessun caso l'utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list).

Le caselle di posta individuali hanno validità pari alla durata della sua identità digitale.

L'utente è tenuto ad adottare gli accorgimenti di seguito indicati, per garantire da un lato la riservatezza di eventuali comunicazioni personali ma al contempo la continuità aziendale e/o l'eventuale esigenza giudiziaria o aziendale di verifica che renda necessaria l'apertura dello strumento di posta:

- cancellare i messaggi a contenuto personale;

(OMISSIS)

Ai fini della sicurezza della rete aziendale, è necessario valutare l'affidabilità del mittente prima di accedere ai file allegati alla posta elettronica (non eseguire download di file eseguibili o documenti da siti Web o Ftp ambigui o comunque non conosciuti il cui indirizzo internet è inserito nel corpo della mail).

Al fine di ridurre il rischio di diffusione di mail contenenti malware vengono applicati alla mail in ingresso filtri di controllo delle estensioni di allegati (es .zip, .rar .exe, etc) e filtri di limitazione anti-spam.

Eventuali segnalazioni di mail ritenute sospette devono essere inoltrate al gruppo di gestione della posta elettronica.

In Ateneo è attivo il tracciamento dei log di posta, per le seguenti finalità: ragioni di sicurezza interna, statistiche, prevenzione dei reati, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta. L'Ateneo assume come tempo di conservazione per questa tipologia di log 6 mesi.

Il contenuto dei messaggi inviati deve essere espresso in maniera professionale e corretto per non arrecare danno alla reputazione dell'Ateneo. Quindi non devono contenere espressioni che possano rivelarsi offensive, razziste, sessiste, discriminatorie o volgari.

L'Ateneo può intervenire ed accedere alla posta dell'utente solamente in casi eccezionali quali decesso *(OMISSIS)*, richieste delle autorità giudiziarie; controlli, previa informativa fornita *(OMISSIS)* e nel rispetto del principio di trasparenza, possono essere consentiti per:

- finalità di sicurezza (d.r. nei limiti individuati dal Garante Privacy) o, qualora sussistano fondati sospetti nei confronti del dipendente infedele, come necessaria fase di ricerca delle prove della sua colpevolezza;
- sussista l'urgenza di accertare un comportamento lesivo estraneo all'adempimento delle obbligazioni lavorative;

- se le verifiche sono dirette ad accertare comportamenti illeciti e lesivi del patrimonio e dell'immagine aziendale.

(OMISSIS)

Per gli studenti l'account di posta verrà disabilitato dopo 18 mesi dal conseguimento del titolo oppure dopo 3 mesi nel caso in cui non vi sia più una carriera attiva. In entrambi i casi, contestualmente alla disattivazione dell'account verrà cancellato l'account istituzionale (xyz@edu.unito.it).

5. La Rete dell'Ateneo

La rete di Ateneo è dedicata esclusivamente alle attività istituzionali.

È pertanto vietato:

- l'utilizzo per finalità private o che ne pregiudichino le funzionalità
- la connessione a reti esterne di altri gestori (salvo eccezioni autorizzate dalla Direzione Sistemi Informativi, Portale, E-learning)
- la connessione di apparati di rete o di connettività non autorizzati (es: hub, switch o router di qualsiasi tipo; Access Point o hotspot etc…).

La gestione, lo sviluppo, il monitoraggio, la sicurezza della rete di Ateneo sono di pertinenza esclusiva della Direzione Sistemi Informativi, Portale, E-learning: qualunque azione promossa da strutture locali deve necessariamente essere autorizzata e condivisa con la stessa.

L'accesso e l'utilizzo della rete di Ateneo comportano l'accettazione delle specifiche e delle condizioni fin qui esposte e la consapevolezza che sistemi automatizzati conservano alcuni dati della navigazione Internet (cosiddetti file di log) per un periodo non superiore ai 6 mesi per scopi di gestione della sicurezza informatica e del monitoraggio del servizio, così come esposto nelle informative presenti sul Portale di Ateneo.

Le policy di sicurezza generali implementate sui firewall di Ateneo prevedono l'attivazione di regole di filtro su siti pericolosi (URL filtering), l'attivazione di regole per mitigare attacchi DDoS, e il blocco delle connessioni rilevate come minacce di livello critico. Le policy sono descritte in dettaglio nei documenti contenuti nella Intranet.

Le regole di visibilità fra i vari servizi di rete – ad esempio fra le reti dedicate al wifi o alle aule di didattica ed il resto della rete di Ateneo – sono elencate in dettaglio nei documenti che descrivono i servizi singoli.

I criteri adottati per il controllo dell'accesso in rete di tutti i dispositivi sono descritti nel documento sul progetto di Ateneo 802.1x, presente anch'esso nella Intranet.

5.1 Accesso alla rete GARR

L'Ateneo di Torino fa parte del Consortium GARR, ovvero la rete italiana delle Università e degli Enti di Ricerca. Il GARR fornisce all'Ateneo servizi di collegamento e di interoperabilità che permettono di accedere alla rete Internet.

L'utilizzo della rete di Ateneo è pertanto subordinato al rispetto da parte di tutti gli utenti delle linee guida e delle norme di accesso e di utilizzo adottate dal Consortium GARR in aggiunta all'osservanza del presente Regolamento.

Le policy sull'utilizzo della rete del GARR sono reperibili al seguente link http://www.garr.it/a/utenti/regole-di-accesso/acceptable-use-policy-aup.

(OMISSIS)

6. Aule informatiche e laboratori virtualizzati

Le aule ed i laboratori devono prevedere la separazione della porzione di rete in uso alle aule dal resto della rete di Ateneo con la quale non possono comunicare se non per accedere ai servizi centrali o alle funzionalità multimediali.

L'uso delle postazioni da parte di ciascun utente è consentito solo previa autenticazione che avviene secondo quanto descritto nel paragrafo sulle identità digitali.

Dove le aule sono configurate con thinclient, i terminali si devono collegare a macchine virtuali che accedono ad Internet tramite NAT (network address translation) e il traffico è consentito soltanto per i protocolli web (HTTP / HTTPS). La sessione di lavoro viene cancellata al termine di ogni utilizzo ed i desktop virtualizzati vengono resettati.

Dove le aule sono dotate di personal computer sono configurate per gestire le postazioni nel dominio Ateneo.
L'inserimento in dominio permette il controllo delle policy di sicurezza descritte ai paragrafi relativi alle postazioni di lavoro.

7. Laboratori di ricerca

Nei laboratori di ricerca viene fornita la connettività dalla Direzione competente per i sistemi informativi. La responsabilità sugli apparati/computer/server contenuti nei laboratori (luoghi ai sensi del D.M 363/98 o ambienti in cui si svolgono attività didattica, di ricerca o di servizio che comportano l'uso di macchine, di apparecchi ed attrezzature ·di lavoro, di impianti, di prototipi o di altri mezzi tecnici, ovvero di agenti chimici, fisici o biologici. Sono considerati · laboratori, altresì, i luoghi o gli ambienti ove si svolgono attività al di fuori dell'area edificata della · sede -quali, ad esempio, campagne archeologiche, geologiche, marittime")

e la gestione degli stessi compete al Direttore del Dipartimento o agli amministratori di sistema individuati dallo stesso (nel dipartimento o anche nell'ambito di un dipartimento afferente allo stesso polo previo accordo fra direttori di dipartimento o in casi particolari con il direttore per i sistemi informativi) ed al responsabile del progetto.

La sicurezza informatica relativa al laboratorio di ricerca è di responsabilità del Direttore del Dipartimento o di un suo

delegato se presente e, in relazione ai sistemi presenti, ai singoli amministratori di sistema e responsabili dei progetti scientifici che usano il/i sistemi. Sarà cura del Direttore del Dipartimento nominare, laddove necessario, eventuali amministratori di sistema delle apparecchiature informatiche presenti nei laboratori.

L'Amministrazione si riserva di intervenire a supporto dei direttori di dipartimento per la definizione dei sistemi e dei relativi amministratori comprese le eventuali iniziative informative/formative.

8. Servizi multimediali

Gli impianti audio/video delle aule o delle sale riunioni collegati in rete, sono attestati su apparati di rete dedicati al servizio multimediale e isolati dal resto del traffico di Ateneo. Dalla rete riservata al multimediale non è possibile navigare in Internet.

L'apparato che rappresenta il punto di contatto con la rete di Ateneo è collocato in un rack chiuso a chiave (le chiavi sono a disposizione del solo personale addetto alla gestione/manutenzione).

Le aule in cui sono posizionati i rack sono inoltre accessibili solo per attività autorizzate; devono infatti essere prenotate attraverso un applicativo e l'accesso fisico è controllato dagli addetti alla Logistica.

Le aule predisposte per la trasmissione in streaming consentono l'avvio di questa funzionalità solo attraverso credenziali note al solo personale addetto a questo specifico servizio.

La funzionalità di streaming pubblico sulla piattaforma media.unito.it prevede inoltre che il flusso venga inserito in programmazione attraverso un applicativo web accessibile tramite autenticazione al solo personale addetto.

Per le postazioni di Digital signage si utilizzano configurazioni di rete per impedire che gli apparati vengano sostituiti in modo non autorizzato e che il nuovo apparato possa utilizzare la rete di Ateneo e navigare.

La gestione dei contenuti trasmessi avviene attraverso un applicativo web accessibile tramite autenticazione al solo personale addetto. Le liberatorie per l'uso dei contenuti, immagini etc sono conservate sui sistemi documentali di ateneo disponibili alla redazione web del portale di Ateneo

9. Data center e servizi esterni ed in cloud

Per Data Center si intende uno spazio fisico composto da server, storage, apparati di rete, cablaggi e armadi, sistemi di condizionamento.

L'Ateneo si avvale di alcuni Data Center interni e di altri in Cloud, oppure utilizza gli spazi di consorzi a cui l'università di Torino partecipa.

(OMISSIS)

L'Ateneo utilizza servizi in cloud o servizi realizzati e mantenuti da società esterne

(OMISSIS)

In via esemplificativa e non esaustiva:

- Cineca - Consorzio Interuniversitario per i dati degli studenti, personale, imprese e fornitori

L'Università di Torino utilizza servizi informatici ed infrastrutture ICT di Cineca per la gestione della didattica, della ricerca, della contabilità, della gestione elettronica dei documenti, del Portale, dell'App MyUniTO + e di altri servizi accessori per il funzionamento dei sistemi.

- Google LLC - per i dati degli studenti e del personale
  L'Università di Torino utilizza la soluzione per il settore educational di Google per la posta elettronica istituzionale del personale e degli studenti, il sistema analitycs per la gestione delle statistiche dei siti web dell'Ateneo e le soluzioni per la collaboration on line (drive, ecc) e le per le mappe interattive.
- Microsoft Corporation – per i dati degli studenti e del personale
  L'Università di Torino utilizza Microsoft Corporation per le soluzioni di office automation del personale e degli studenti.
- CISCO – per i dati degli studenti e del personale
  L'Università di Torino utilizza alcune soluzioni CISCO per il sistema di telefonica VOIP e per il sistema di web conference
- CSI – Piemonte – per i dati del personale
  L'Università di Torino utilizza servizi informatici ed infrastrutture ICT di CSI nell'ambito delle soluzioni disponibili agli atenei consorziati relativamente al personale.

I dati vengono anche comunicati all'esterno dell'Ateneo nei seguenti casi:

- quando le richieste provengono da enti pubblici e i dati richiesti sono necessari all'ente che ne fa richiesta per fini istituzionali (ad esempio, le informazioni scambiate periodicamente con il Ministero dell'Istruzione, dell'Università e della Ricerca, l'Anagrafe Nazionale degli Studenti, il Ministero delle Finanze, il Ministero degli Affari Esteri, l'Ente Regionale per il Diritto allo studio universitario, l'Istat, il Cnvsu, l'Osservatorio Regionale per l'Università e per il diritto allo studio Universitario, il Centro per l'impiego)
- quando le richieste provengono dall'autorità giudiziaria
- al momento dell'esame di laurea alcuni dati potrebbero essere trasmessi ad aziende o enti che ne facciano richiesta e che dichiarino di utilizzarli solo per attivare eventuali rapporti di lavoro o pubblicizzare attività formative e culturali.

Per le **modalità di trattamento**, i **tempi di conservazione**, l'eventuale **trasferimento verso Paesi extraUE** si rimanda alle informative privacy specifiche dei singoli servizi

9.1 Politiche di backup e recovery

Il backup di tutti i sistemi vengono effettuato giornalmente con una conservazione (retention) di almeno 30 giorni. Il sistema utilizzato per il backup risiede in un luogo diverso dai Data Center ove sono collocati i server, in modo da garantire la disponibilità del backup in caso di guasto. Periodicamente è effettuato il recovery di test dei sistemi come prassi di verifica.

Tutti i servizi che si ritengono critici prevedono dinamiche di Disaster Recovery gestiti dalla direzione competente per i sistemi informativi o dai singoli fornitori dei servizi.

(OMISSIS)

10. Policy per interventi di sicurezza e controlli

La Direzione competente per i sistemi informativi opera con funzioni di monitoraggio sulla implementazione delle regole di sicurezza informatica. Per tale motivo il personale tecnico afferente alla Direzione competente per i sistemi informativi è autorizzato a compiere interventi tecnici e/o manutentivi diretti a garantire la sicurezza e la salvaguardia del sistema (es. attività di controllo, amministrazione e backup, ecc).

(OMISSIS)

Il personale autorizzato dalla Direzione competente per i sistemi informativi può in qualunque momento procedere alla rimozione di file, applicazioni, software o altro che riterrà pericoloso per la sicurezza dell'Ateneo.

(OMISSIS)

Vengono inoltre effettuati controlli difensivi atti a limitare la diffusione di malware all'interno della rete aziendale o altri problemi di sicurezza informatica. Per tali fini, nel caso in cui emergano anomalie, vengono effettuate attività di verifica su alcune tipologie di log, tracciati dai sistemi di protezione, quali:

- i dati rilevati dalle console dei sistemi antivirus (numero infezioni, tipologia, pc infettati, user di appartenenza, etc)
- i log di posta e i log derivanti dalla applicazione dei mail filtering (caselle di destinazione/arrivo messaggi, ora/minuti invio/ricezione, tipologia di file allegato, user, ad esclusione dei contenuti della posta)
- log dei sistemi di URL Filtering e Content Filtering (tracciatura delle URL permesse/bloccate dalle policy aziendali, tracciatura della connessione proveniente dagli IP/user, ora/minuto/secondo, server acceduto, pagina visitata, dimensioni file scaricato, numero di accessi continuativo)
- log DLP (analisi delle tracciature dei documenti riservati acceduti; ora/minuto/secondo, tipologia di regola di controllo, IP/user che ha effettuato l'azione)
- log di accesso ai database o ai server aziendali.

(OMISSIS)

Glossario

Amministratore di sistema: *la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi compresi gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi*;

Autenticazione informatica: *l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità*;

Autorizzato al trattamento: *le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile*;

Backup: *Copia di dati ridondante effettuata, in modo sistematico e automatico, in modo da salvaguardarne la disponibilità e l'integrità.*

Banca dati: *insieme di grandi quantità di informazioni tra loro omogenee, registrate in una memoria di massa, gestite da un apposito programma e strutturate in modo tale da facilitarne la consultazione da parte di uno o più utenti*

CERT-GARR: *è un servizio operativo del GARR la gestione degli incidenti di sicurezza informatici in cui siano coinvolti enti collegati alla rete GARR*

Client: *qualsiasi computer (di prestazioni generalmente medio-basse) che possa accedere a risorse o servizi erogati da un server tramite connessione di rete.*

Cloud: *insieme di dati e servizi accessibili, tramite credenziali specifiche, da qualunque luogo, tramite qualsiasi connessione.*

Credenziali di autenticazione: *i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica*;

Data Center: *si intende uno spazio fisico composto da server, storage, apparati di rete, cablaggi e armadi, sistemi di condizionamento*

Dati giudiziari: *sono quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti. Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato*;

Dati identificativi: *i dati personali che permettono l'identificazione diretta dell'interessato*;

Dati personali: *qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*;

Dati particolari: *i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*;

Defacing (di un sito web): *M*odifica/sostituzione non autorizzata della home page o di una delle pagine interne di un

sito web.

DPO: Data Protection Officer ovvero Responsabile Protezione Dati

Firewall: *Soluzione tecnica (software o dispositivo fisico) che permette di monitorare e filtrare il traffico in ingresso in una data rete*

GARR: *Gruppo per l'Armonizzazione delle Reti della Ricerca è il nome della rete italiana a banda ultralarga dedicata alla comunità dell'istruzione, della ricerca e della cultura.*

Hacker: *Esperto informatico in grado di introdursi in reti e sistemi di computer senza autorizzazione, con scopi essenzialmente dimostrativi.*

Host: *calcolatore sul quale sono memorizzate le informazioni*

Interessato: *la persona fisica cui si riferiscono i dati personali*;

Internet: Rete planetaria, ad accesso pubblico. Le risorse possono essere condivise, a livello globale, tra le reti locali e computer singoli. Internet è la "rete delle reti".

Malware *(Malicious software): qualsiasi software che, una volta installato in un sistema, possa produrre effetti dannosi per il sistema stesso (pc, notebook, telefoni, …) o per i documenti contenuti in esso.* L'installazione di questo tipo di software avviene in modo inconsapevole o ingannevole.

Patch: programma *o file per la correzione di bug scoperti in pacchetti software.*

Phishing: *Attività, volta a carpire informazioni personali o codici di accesso (ad esempio possono venire inviate e-mail in modo massivo contando sul fatto che qualche destinatario resti vittima dell'inganno. La maggior parte di queste comunicazioni vengono, in genere, intercettate dai servizi automatici anti-spam dei provider che forniscono servizi di posta elettronica).*

Rete locale: *(LAN, Local Area network): infrastruttura informatica costituita da diversi computer (in genere server e client) connessi tra loro e che comunicano tramite regole prestabilite (l'insieme di regole è detto "protocollo"). I client possono usufruire di risorse e servizi centralizzati (architettura client-server).*

Ransomware: *Particolare tipo di malware che blocca il sistema oggetto di infezione o che ne rende inutilizzabili (tramite cifratura) i documenti prodotti dall'utente. Lo sblocco del sistema o la decifrazione dei documenti può avvenire dietro pagamento di un 'riscatto' (in inglese, 'ransom'). Un famigerato esempio di questo tipo di minaccia è il ransomware Cryptolocker.*

Server: *Computer ad elevate prestazioni in grado di fornire servizi ed accesso dati ad altri computer (che non necessito di particolari risorse hardware), denominati "client".*

Social engineering: *(Ingegneria sociale, in ambito di sicurezza informatica): studio del comportamento individuale di una persona al fine di carpire informazioni utili per un attacco informatico.*

Spear phishing: *Attività di phishing diretta, in modo deliberato, ad un soggetto in particolare.*
Spyware: *Malware volto a registrare informazioni inerente all'attività dell'utente in rete.*

Responsabile del trattamento: *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*;

Strumenti elettronici: *gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento*;

Titolare del trattamento: *la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*;

Trattamento: *qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*;

URL filtering: *è un componente software progettato per limitare l'accesso a siti Web che contengono malware.*

Violazione di dati personali: *violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico*.

Virus. *Malware che, una volta eseguito, infetta altri file in modo da generare copie di sé stesso.*