ISTITUTO COMPRENSIVO "Ignazio Silone"
Via Alessandro Torlonia 108 B - 67056 LUCO DEI MARSI - Telefono 086352117
Codice Fiscale 81006290662 – Codice Meccanografico AQIC82100B
Mail Ministeriale aqic82100b@istruzione.it – Pec AQIC82100B@PEC.ISTRUZIONE.IT
http://www.scuolelucodeimarsi.edu.it - Codice Univoco IPA: UFOJ2T

ISTITUTO COMPRENSIVO - "IGNAZIO SILONE"-LUCO DEI MARSI
Prot. 0009204 del 14/11/2025
I-4 (Uscita)

DISCIPLINARE TECNICO per l'utilizzo degli strumenti informatici e principali misure di sicurezza

ai sensi del Regolamento UE 679/2016 e dei Provvedimenti del Garante per la protezione dei dati personali rilevanti e ai sensi delle Misure minime di sicurezza per le PA di Agid (Livello M-S).

SOMMARIO

INTRODUZIONE **4**
PREMESSA **4**
FINALITA' DEL DOCUMENTO E MODALITA' DI APPROVAZIONE **5**
RIFERIMENTI NORMATIVI **5**
MATRICE DELLA REDAZIONE E DELLE REVISIONI **7**
RISORSE DELL'ENTE E GESTIONE DELL'ACCESSO AI SISTEMI INFORMATICI E TELEMATICI **7**
DISPONIBILITÀ DELLE RISORSE DELL'ENTE **7**
SISTEMI DI AUTENTICAZIONE E GESTIONE DELLE CREDENZIALI DI ACCESSO A SISTEMI INFORMATICI **7**
GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE ALLE RISORSE INTERNE 7
Scelta della password 8
Conservazione della password 9
GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE GENERATE DA INFOCAMERE 10
PROTEZIONE DEGLI STRUMENTI AZIENDALI **10**
PROTEZIONE DELLA POSTAZIONE DI LAVORO **10**
SISTEMI DI SALVATAGGIO DEI DATI **10**
SISTEMI ANTINTRUSIONE **10**
UTILIZZO DELLE RISORSE DI SISTEMA **11**
ARCHIVI INFORMATICI CONTENENTI DATI PARTICOLARI (EX "DATI SENSIBILI") **11**
INSTALLAZIONE DI SOFTWARE **11**
UTILIZZO DI ULTERIORI DISPOSITIVI E STRUMENTI AZIENDALI **12**
DISPOSIZIONI GENERALI **12**
Computer portatili 11
Stampanti 12
Tablet 12
Telefoni cellulari (smartphone) 12
Dispositivi di firma digitale (o CNS – Carta nazionale dei servizi) 12
Webcam 13
CUSTODIA E PROCEDURE IN CASO DI MALFUNZIONAMENTO, DANNEGGIAMENTO, SMARRIMENTO O FURTO **14**
Malfunzionamento e danneggiamento 14
Smarrimento o furto 14
PROCEDURE IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO **14**
UTILIZZO DI INTERNET E DELLA POSTA ELETTRONICA **15**
UTILIZZO DI INTERNET **15**
UTILIZZO DELLA POSTA ELETTRONICA ISTITUZIONALE **15**
DISATTIVAZIONE DELLA CASELLA DI POSTA ELETTRONICA **16**
CONTINUITÀ DELLE COMUNICAZIONI **16**

POSTA ELETTRONICA PERSONALE 17
CANCELLAZIONE, RIASSEGNAZIONE E SMALTIMENTO DEI SUPPORTI DI MEMORIZZAZIONE 17
SISTEMA DI MONITORAGGIO E AUDIT 17
VERIFICHE SU LOG E POSTA ELETTRONICA 18
VERIFICHE SUI LOG 18
Log di sistema 18
Log di navigazione 19
Conservazione dei dati di log 19
ACCESSO ALLE EMAIL ISTITUZIONALI 20
FORMAZIONE 20
CONTROLLI E SANZIONI 20
MODALITA' DEI CONTROLLI 20
SANZIONI 21
DISPOSIZIONI FINALI 21
INTERPRETAZIONE, MODIFICHE E DEROGHE 21
Interpretazione 21
Modifiche e deroghe 21

INTRODUZIONE

PREMESSA

L'ampia diffusione delle tecnologie dell'informazione avvenuta nel corso degli ultimi anni ha rappresentato sicuramente un traguardo importante per il mondo del lavoro. Tuttavia, accanto ai benefici generati da tali tecnologie, occorre contemperare le esigenze organizzative del datore di lavoro con quelle di tutelare la riservatezza dei dati personali dei lavoratori.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'ente stesso a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile. I controlli sull'uso degli strumenti informatici/telefonici tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dalla disciplina sul trattamento e la tutela dei dati personali.

In considerazione di ciò, e sollecitato da diverse segnalazioni, il Garante per la protezione dei dati personali ha avvertito la necessità di predisporre delle linee guida per i datori di lavoro pubblici e privati, affinché prevedessero un'apposita disciplina interna per l'utilizzo dei dispositivi tecnologici da parte dei lavoratori[1].

Gli obiettivi che il Garante si è prefisso attraverso l'elaborazione di tali linee guida sono molteplici. Da un lato si auspica la predisposizione, da parte dei datori di lavoro, di regole interne volte alla definizione delle modalità di utilizzo delle tecnologie informatiche da parte dei lavoratori[2]. Dall'altro lato, le linee guida si propongono di soddisfare esigenze di tutela dello stesso lavoratore o dei terzi, contro le condotte dei datori di lavoro che si traducano in una violazione della riservatezza. In considerazione dei peculiari riconoscimenti che il nostro ordinamento assegna al luogo di lavoro, il Garante ha ritenuto imprescindibile stabilire specifiche regole a presidio della integrità della *privacy* del lavoratore[3].

Il Garante nella Newsletter n. 424 del 17 febbraio 2017, per es., ha ribadito che l'accesso in maniera indiscriminata, da parte del datore di lavoro, alla posta elettronica o ai dati personali contenuti negli *smartphone* in dotazione al personale costituisce un comportamento illecito. Nel disporre il divieto l'Autorità ha affermato che il datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione professionale ed il rispetto delle Linee Guida per l'utilizzo dei sistemi e dei servizi informatici aziendali da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità, attenendosi ai limiti previsti dalla normativa. La disciplina di settore in materia di controlli a distanza, inoltre, non consente di effettuare attività idonee a realizzare, anche indirettamente, il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore.

Più recentemente, il Garante con la Newsletter n. 437 del 26 gennaio 2018 ha dichiarato la legittimità dei controlli effettuati da parte del datore di lavoro sui consumi telefonici connessi alle SIM aziendali in presenza di alcune condizioni: in particolare, deve assicurare che il *file* sul quale sono memorizzati i dati estratti dal portale del gestore del servizio di connessione del telefono sia protetto mediante opportune tecniche di cifratura e fare sì che, nelle successive rielaborazioni dei dati, questi siano anonimizzati mediante l'utilizzo di tecniche che non consentano la re-identificazione dell'interessato.

Tanto premesso è stato elaborato il presente Disciplinare per:

- indicare i criteri per il corretto utilizzo degli strumenti informatici/telefonici da parte dei dipendenti e/o collaboratori;
- definire i limiti e le finalità entro i quali il datore di lavoro (titolare del trattamento) può legittimamente porre in essere controlli sui predetti strumenti;
- rilasciare ai dipendenti un insieme di istruzioni valide anche ai sensi dell'art. 32, par. 4 del Regolamento UE 679/2016.

[1] Deliberazione del Garante, 1 marzo 2007, n. 13, punto 1.1.
[2] Deliberazione del Garante, 1 marzo 2007, cit., punto 1.1 lett. a).
[3] Deliberazione del Garante, 1 marzo 2007, cit., punto 1.2.

La regolamentazione di seguito proposta, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stata redatta tenendo conto, da una parte, delle disposizioni contenute nella Legge n. 300/1970 in tema di controllo dei lavoratori (art. 4) e di provvedimenti disciplinari (art. 7) e, dall'altra, delle indicazioni emerse nelle sentenze di merito e di legittimità rinvenibili in materia. Vengono inoltre considerati gli specifici obblighi previsti dal Regolamento (UE) 2016/679, e dalla disciplina nazionale in materia di *privacy*, oltre che le norme in materia di sicurezza sul lavoro (D.Lgs. n. 81/2008 ed Allegato XXXIV).

L'Istituto è tenuto, inoltre, ad uniformarsi a quanto previsto nelle Misure Minime di Sicurezza ICT previste da AGID.
Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti
Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.
A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo **tre livelli di attuazione.**
Minimo (M): è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.
Standard (S): è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.
Avanzato (A): deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.
Le misure minime sono un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento.
Le misure minime: forniscono un riferimento operativo direttamente utilizzabile (checklist), stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili; forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento; responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.
L'adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017.
Secondo la circolare, le misure minime di sicurezza devono essere adottate da parte di tutte le pubbliche Amministrazioni entro il 31 dicembre 2017.

Scopo del presente documento, dunque, è **informare i dipendenti della Istituto in merito ai propri diritti e ai propri doveri circa l'utilizzo delle tecnologie dell'informazione messe a disposizione dall'istituto per lo svolgimento dell'attività lavorativa**.

È quindi necessario che ciascun dipendente si adegui al rispetto delle regole riportate nel presente documento, al fine di preservare la riservatezza dei propri dati e, al contempo, permettere all'Istituto la tutela dei propri interessi.

FINALITA' DEL DOCUMENTO E MODALITA' DI APPROVAZIONE

In attuazione degli specifici obblighi formali e sostanziali proposti dal Regolamento UE 679/2016 (di seguito anche "GDPR"), dal D.Lgs. n. 196/2003, recante il Codice in materia di protezione dei dati personali, come modificato dal D.Lgs.
n. 101/2018 (di seguito anche "Codice") e da specifici provvedimenti del Garante per la protezione dei dati personali (di seguito indicato anche "Garante"), si comunica a tutti i dipendenti e collaboratori dell'Istituto il presente "Disciplinare sull'utilizzo degli strumenti informatici e delle misure di sicurezza".
Scopo del presente documento è definire i comportamenti da adottare e le regole di sicurezza da seguire al fine di:

- ✓ garantire nel tempo – attraverso idonee misure di sicurezza - il livello di riservatezza, integrità e disponibilità dei dati personali richiesto dalla normativa vigente e, più in generale, delle informazioni raccolte e gestite dall'Istituto in qualità di Titolare/Contitolare o Responsabile del trattamento (in relazione ad attività svolta con altri Enti);
- ✓ assicurare la funzionalità e il corretto utilizzo degli strumenti messi a disposizione dei lavoratori;
- ✓ salvaguardare il patrimonio dell'istituto.

Le prescrizioni contenute nel Disciplinare:

a) devono essere conosciute e condivise quali **norme di comportamento durante lo svolgimento delle attività lavorative**, ognuno per la propria AOO-UOR/Servizio/Ufficio e per le mansioni di competenza. Il rispetto del Disciplinare costituisce un elemento per l'implementazione ed il mantenimento di un idoneo sistema di gestione sicura dei dati e delle informazioni;
b) devono intendersi quali **istruzioni impartite dal Titolare** obbligatorie con decorrenza dalla data della sua entrata in vigore e con valore di ordine di servizio, il cui mancato rispetto **costituisce inosservanza delle disposizioni al personale** e può essere, quindi, oggetto di provvedimenti disciplinari ai sensi della vigente normativa contrattuale e del Codice disciplinare dell'Ente Camerale;
c) **integrano e completano, infine, l'informativa per il trattamento dei dati personali** ai fini di gestione del rapporto di lavoro/collaborazione, redatta e già fornita agli interessati ai sensi dell'art. 13 del GDPR.

Il documento è diffuso a tutto il personale attraverso:

- pubblicazione sulla rete locale VLAN dell'Istituto;
- specifici interventi formativi ed informativi.

RIFERIMENTI NORMATIVI

Il presente documento risponde ai seguenti requisiti normativi:

1. Regolamento UE 679/2016, Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
2. D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali;
3. L. 20 maggio 1970, n. 300, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento;
4. L. 23 dicembre 1993 n. 547, Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;
5. D.L. 27 luglio 2005, n. 144, convertito con la L. 31 luglio 2005 n. 155, Misure urgenti per il contrasto del terrorismo internazionale; Decreto Interministeriale del 16 agosto 2005 (in G.U. n. 190 del 17 agosto 2005);
6. Art. 24 della L. 20 novembre 2017, n. 167, Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017;
7. L. 22 aprile 1941 n. 633, Protezione del diritto d'autore e di altri diritti concessi al suo esercizio [*al cui interno è compresa la disciplina dei programmi per elaboratori e le banche dati*];
8. D.Lgs. 10 febbraio 2005, n. 30, Codice della proprietà industriale;
9. D.Lgs. 1 agosto 2003, n. 259, Codice delle comunicazioni elettroniche;
10. D.Lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale;
11. D.P.R. 16 aprile 2013, n. 62, Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165;
12. Codice di comportamento dei dipendenti della Camera di Commercio di Latina, approvato con provvedimento della Giunta Camerale n. 62, del 21.11.2013
13. Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica, Direttiva 26 maggio 2009, n. 2, Utilizzo di Internet e della casella di posta elettronica istituzionale sul posto di lavoro;
14. Garante per la protezione dei dati personali, Provvedimento del 13 ottobre 2008, Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali;
15. Garante per la protezione dei dati personali, Provvedimento del 27 novembre 2008, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
16. UNI EN ISO 9001:2015 "Sistemi di gestione per la Qualità - Requisiti".

Ulteriori provvedimenti ed indicazioni del Garante che delineano il contesto di riferimento in materia sono:

- Deliberazione n. 13 dell'1 marzo 2007, Linee guida del Garante per posta elettronica e *internet* (G.U. n. 58 del 10 marzo 2007);
- Deliberazione n. 23 del 14 giugno 2007, Linee guida del Garante in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (G.U. n. 161 del 13 luglio 2007);
- Provvedimento del 17 gennaio 2008 in tema di sicurezza dei dati di traffico telefonico e telematico (G.U. n. 30 del 5 febbraio 2008);
- Provvedimento del 24 luglio 2008 in tema di sicurezza dei dati di traffico telefonico e telematico (G.U. n. 189 del 13 agosto 2008);
- Vademecum relativo alle regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati, pubblicato dal Garante il 24 aprile 2015 (https://www.lavoroediritti.com/wp-content/files/Privacy_e_lavoro_-_vademecum_2015.pdf);
- Provvedimento n. 456 del 30 luglio 2015, relativo al trattamento effettuato sulle e-mail di dipendenti ed ex dipendenti;
- Provvedimento n. 547 del 22 dicembre 2016, relativo all'accesso da parte del datore di lavoro alla posta elettronica dei dipendenti;
- Newsletter n. 424 del 17 febbraio 2017, relativa relativo all'accesso da parte del datore di lavoro alla posta elettronica ed agli smartphones dei dipendenti (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5989944#1);
- Newsletter n. 430 del 24 luglio 2017, relativa all'accesso da parte del datore di lavoro *all'*uso privato dei social network e le comunicazioni dei lavoratori, spazi riservati sul cloud (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6633587#3);
- Newsletter n. 437 del 26 gennaio 2018, relativa alla legittimità da parte del datore di lavoro del controllo sui telefoni aziendali dei dipendenti (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7570001#3).

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione

RISORSE DELL'ENTE E GESTIONE DELL'ACCESSO AI SISTEMI INFORMATICI E TELEMATICI

DISPONIBILITÀ DELLE RISORSE DELL'ISTITUTO

Le risorse di calcolo, memorizzazione e trasmissione[4], nonché i relativi strumenti assegnati ai dipendenti o collaboratori sono di proprietà dell'Istituto.

Tali risorse ed i relativi strumenti sono affidati ai dipendenti e collaboratori, in uso NON ESCLUSIVO e temporaneo, per lo svolgimento delle attività di lavoro dell'Ente, nell'esercizio e nei limiti dei compiti e delle mansioni affidate e tenuto conto dei doveri d'ufficio.

È fatto obbligo ai dipendenti e collaboratori di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa, ispirati ai principi della diligenza e correttezza ed idonei a non causare danni o pericoli ai beni mobili, agli strumenti ad essi affidati, nonché ai dati ed informazioni che essi processano [5].

In particolare, il dipendente o collaboratore è tenuto:

- a custodirli in modo appropriato, secondo le indicazioni fornite dall'Istituto;
- ad impiegarli unicamente per finalità inerenti al rapporto di lavoro in relazione alle mansioni assegnate;
- a segnalarne, al competente Ufficio, il furto, il danneggiamento o lo smarrimento.

L'utilizzo di strumenti aziendali per fini che non rientrano tra i compiti lavorativi è occasionalmente tollerato solo nella misura in cui non interferisca con i propri doveri d'ufficio e purché non comprometta l'utilizzo delle risorse e la sicurezza complessiva del patrimonio aziendale (beni, strumenti, dati ed informazioni), nonché i diritti e le libertà degli interessati cui gli eventuali dati personali si riferiscono.

L'utilizzo per finalità istituzionali di strumenti informatici di proprietà di dipendenti e collaboratori è consentito previa autorizzazione specifica del Titolare, o di suoi delegati, che provvederanno – con l'ausilio tecnico dell'Amministratore di Sistema e del Titolare del trattamento dati – a valutarne il livello di sicurezza ai fini dell'eventuale trattamento dei dati personali fornendo, se necessario, le relative soluzioni tecniche.

SISTEMI DI AUTENTICAZIONE E GESTIONE DELLE CREDENZIALI DI ACCESSO A SISTEMI INFORMATICI

GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE ALLE RISORSE INTERNE

Tutti gli utenti a cui vengono forniti accessi alla rete ed alle risorse informatiche dell'Istituto devono essere riconosciuti ed identificabili (Misure Minime di sicurezza AGID ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI).

[4] Nel dettaglio: apparati hardware (postazioni di lavoro, dispositivi portatili, tablet, telefono aziendale), software, supporti ottici e magnetici (es., hard-disk esterni, cd-dvd rom, pen drive, etc.); servizi di collegamento telematico e di gestione della rete; servizi applicativi e tutti quegli strumenti di interoperabilità (ad es., email, sito internet ed intranet) che permettono ai soggetti autorizzati di accedere alla rete e di comunicare tra di loro.

[5] Cfr. la Direttiva *Utilizzo di Internet e della casella di posta elettronica istituzionale sul posto di lavoro*, cit. in premessa.

La gestione delle credenziali e l'accesso ai servizi di rete e di sistema cui l'utente è abilitato in base al proprio profilo di autorizzazione (tale profili sono/potrebbero essere attivati centralmente tramite active directory). In particolare, il sistema di autenticazione è impostato in modo da:

- non attribuire agli account *utente* i privilegi di *amministratore* della macchina (ad eccezione dei soggetti cui è formalmente attribuito il ruolo di amministratore di sistema);
- non consentire l'attivazione di *User ID* già assegnate ad altri incaricati, neppure in tempi diversi;
- segnalare al primo utilizzo e, in seguito ogni 180, giorni che è necessario cambiare la password; in caso di mancata variazione della password, l'account si disabilita fino al rinnovo della stessa;
- consentire all'utente, tramite appositi comandi, il cambio della password anche con una frequenza maggiore rispetto alla scadenza predefinita;
- verificare positivamente i seguenti criteri di composizione delle password:

REQUISITO	DESCRIZIONE
LUNGHEZZA MINIMA	14 caratteri
COMPLESSITÀ	La password deve contenere caratteri appartenenti alle seguenti cinque categorie: • caratteri maiuscoli dell'alfabeto (A -Z). • caratteri minuscoli dell'alfabeto (a -z). • 10 cifre di base (0 - 9). • non alfanumerici (ad esempio, !, $, # o %). • caratteri Unicode[7]. (ad esempio caratteri speciali *, [, !, @) La password non contiene tre o più caratteri del nome di account dell'utente e non deve mai essere riconducibile alla persona.
CRONOLOGIA	Le ultime 5 (non possono essere riutilizzate)
MODIFICA	Ogni 180 gg

Tali requisiti di sicurezza, ove non gestiti centralmente ed automaticamente dal sistema in utilizzo, dovranno essere rispettati autonomamente da tutti i dipendenti e collaboratori che dispongano di utenze istituzionali. (Misure Minime di Sicurezza ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE)

Le credenziali di autenticazione (combinazione tra User ID e password) sono strettamente personali e non devono mai essere divulgate ad altre persone. In proposito, per effetto dell'attribuzione univoca di credenziali di accesso ed autorizzazione a risorse aziendali, il dipendente è consapevole che **qualsivoglia atto, azione e/o fatto operato all'interno del Sistema con i codici identificativi o dopo l'accesso al Sistema stesso attraverso l'utilizzo di detti codici sarà inequivocabilmente attribuito al soggetto cui le credenziali si riferiscono**.

Nel caso in cui si abbia il dubbio che la propria password sia stata violata - ovvero un soggetto abbia effettuato un accesso abusivo al sistema - è fatto obbligo agli utenti di avvertire immediatamente gli amministratori di sistema, che provvederanno ad attivare le verifiche del caso (anche mediante analisi dei log di accesso) ed eventualmente a resettare la password al fine di consentire all'utente di impostarne una nuova e sicura.

Come previsto nell'analisi dei rischi redatta in attuazione dell'art 32 del GDPR679/2016 è stata individuata la figura di custode delle password che è tenuto alla redazione ed all'aggiornamento dell'apposito registro di cambio password. Ad ogni cambio password l'utente è tenuto ad inserirla in busta chiusa, firmare la busta chiusa sui lembi e consegnarla all'amministrazione di sistema (salvo quanto eventualmente disposto in maniera diversa per opportuna attivazione/configurazione del servizio centralizzato active directory)

L'Amministratore di Sistema provvede a disabilitare le utenze il cui titolare abbia cessato il rapporto di lavoro o collaborazione con l'Istituto.

[6] Servizio di directory compatibile con lo standard X500 che consente di gestire in modo centralizzato account utenti, applicazioni, servizi, periferiche e tutto ciò che fa parte di un sistema distribuito.
[7] Per caratteri Unicode (nell'ambito di un sistema di codifica – gestito dal Consorzio internazionale Unicode – che assegna un numero univoco ad ogni carattere utilizzato per la scrittura informatica/telematica di testi), con riferimento a quanto indicato, si intendono i c.d. caratteri "speciali" come: ∝; ₭; ₽; ₸; ₰; etc. Cfr. https://unicode-table.com/it/#control-character .

L'obiettivo da perseguire, quando viene scelta una password, è di rendere difficile una sua eventuale ricostruzione e/o individuazione.

La complessità con la quale viene costruita è importante per contrastare le tecniche di bruteforce (forza bruta), che tentano ogni possibile combinazione di lettere, numeri e caratteri per determinare la password utilizzata. Naturalmente una ricerca di questo tipo, persino se processata su un computer capace di generare e testare migliaia di combinazioni al secondo potrebbe, con un'appropriata politica di definizione delle password, richiedere molto tempo. Dunque solo una password correttamente definita e gestita in modo da non essere divulgata può costituire un'appropriata tecnica per il controllo e la discriminazione degli accessi ai sistemi informatici.
Le indicazioni che seguono, se correttamente applicate, costituiscono una *idonea* misura di sicurezza in attuazione delle misure minime di sicurezza AGID punto ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE livelli M ed S e di quanto previsto nell'analisi dei rischi art. 32 GDPR 679/2016

Fermi restando i requisiti di sicurezza impostati come automatici, e comunque per tutti i sistemi che presentano un secondo livello di autenticazione non gestito centralmente, nella scelta della password si raccomanda di:

NON USARE per creare la propria password:
- la User ID in qualsiasi forma (così com'è, invertito, scritto con caratteri maiuscoli, raddoppiato, etc.);
- il nome e/o il cognome dell'utente, neanche se combinato ad altri dati personali;
- altre informazioni che siano facilmente ottenibili conoscendo l'utente a cui è associata la password (ciò include ad es.: numero telefonico, data di nascita, di compleanno, codice fiscale, nome della marca dell'automobile (o la targa), il nome della via di residenza, etc.);
- il nome e/o cognome di parenti (moglie, figli), personaggi pubblici o personaggi dei fumetti (es. pippo, pluto, etc.);
- il nome di mesi, giorni della settimana, stagioni, città, stati;
- una sequenza banale di caratteri (come, ad esempio: aaabbb, qwerty, 123456);
- sigle di funzioni/uffici dell'Ente;
- il nome di progetti e/o dell'applicativo cui la password si riferisce;
- i numeri scritti in cifre;
- stringhe composte da più di 3 caratteri (numerici, alfabetici, speciali) consecutivi uguali;
- con la stessa struttura della password precedentemente utilizzata;
- una qualsiasi password precedentemente menzionata preceduta o seguita da una cifra (es. MarioRossi99 o 99MarioRossi).

USARE per creare la propria password:
- stringhe costruite utilizzando contemporaneamente caratteri alfabetici, numerici e simboli speciali;
- stringhe composte usando contemporaneamente caratteri alfabetici minuscoli e maiuscoli;
- stringhe strutturate con:
  - ✓ un numero di caratteri alfabetici compresi tra 3 e 5;
  - ✓ un numero di caratteri speciali compresi tra 1 e 3;
  - ✓ un numero di caratteri numerici tra 2 e 4;
- la password deve essere comunque definita in modo che l'utente sia in grado di impararla a memoria per evitare che si renda necessario doverla scrivere e/o salvare. Un esempio di password conforme alle indicazioni sopra esposte è la seguente:
  - ✓ **"2Galli+2Galline=4Polli"** dove sono presenti: lettere, numeri, caratteri speciali, lunghezza adeguata, per cui ha una struttura complessa, però è anche semplice da ricordare.

Conservazione della password

Persino avendo scelto una password di difficile violazione per tutelare gli accessi ai sistemi informatici, è comunque consigliabile seguire le successive istruzioni che forniscono indicazioni su come gestire, durante tutto il ciclo di vita, la password di un utente:

- bisogna evitare, per quanto possibile, di inserire le credenziali in presenza di altri soggetti;
- la password, in particolare, deve essere custodita in modo appropriato: non deve mai essere scritta su fogli, biglietti, post-it o su oggetti (unità di memorizzazione rimovibili, sotto la tastiera o mouse, etc.) lasciati nelle vicinanze del computer; inviata per posta elettronica; comunicata a terzi;
- nel caso in cui non si possa fare a meno di annotare le proprie password in forma digitale su file, si raccomanda che questo sia a sua volta opportunamente cifrato dall'utilizzatore (ad es., compressione zip/rar con password non banale);
- in ogni caso è necessario provvedere alla modifica della password se essa sia stata rivelata – pur essendo vietato - ad altri consapevolmente (ad es., per consentire l'accesso momentaneo ad una base di dati in caso di assenza dell'incaricato) o se si sospetta che questo possa essere accaduto accidentalmente.

Com'è noto, l'utilizzo su vari sistemi web oriented (ovvero presenti su Internet) delle medesime credenziali può esporre a compromissione gli stessi sistemi (in quanto le credenziali, una volta carpite su uno di essi potrebbero essere utilizzate anche sugli altri).
In proposito è consigliabile di utilizzare per i sistemi in ambito lavorativo credenziali diverse da quelle utilizzate per sistemi ad uso non lavorativo e privato.

PROTEZIONE DEGLI STRUMENTI AZIENDALI

PROTEZIONE DELLA POSTAZIONE DI LAVORO

In nessun caso bisogna lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali, al fine garantire la protezione delle postazioni di lavoro accese e non utilizzate.

Le istruzioni da seguire in caso di assenza – anche temporanea – dalla postazione di lavoro sono, in ordine decrescente di importanza, le seguenti:

- bloccare la postazione con il comando "blocca computer" attivabile digitando contemporaneamente i tasti CTRL - ALT – CANC ovvero chiudere tutte le applicazioni aperte e le connessioni verso applicazioni remote, quando non più necessarie;
- attivare l'opzione *Screen Saver Lock* (c.d. "screensaver con password"), che blocca la macchina dopo un periodo di inattività (determinato *una tantum* dallo stesso utente) ovvero la disconnessione automatica dal sistema in uso;
- chiudere tutte le applicazioni/finestre aperte avendo cura di eseguire la procedura di logout;
- non rivolgere il monitor verso zone di transito.

In ogni caso è opportuno e fortemente consigliato di chiudere a chiave la porta dell'Ufficio in caso di assenza prolungata di tutti gli incaricati ivi assegnati.

SISTEMI DI SALVATAGGIO DEI DATI

A tutto il personale che, a qualsiasi titolo, presta la propria attività lavorativa presso L'Istituto, viene assegnato uno spazio di lavoro personale e dedicato della rete aziendale (cartelle personali ad accesso esclusivo), spazi di lavoro condivisi a livello di gruppo (cartelle con accesso agli autorizzati) e spazi di lavoro condivisi tra tutti (cartelle con accesso libero) sulla infrastruttura di rete localizzata presso l'Istituto , disponibili per il salvataggio di tutti i database (da intendersi anche come cartelle di file).

Lavorare esclusivamente in rete e non in locale e, di conseguenza, il salvataggio dei dati in queste cartelle costituisce una fondamentale regola di prudenza, in quanto su queste risorse vengono gestite centralmente ed automaticamente specifiche politiche di back-up secondo la disciplina tecnica vigente.

Le politiche di back-up e di sicurezza sono sottoposte a costante valutazione ed aggiornamento dovuta alla corretta applicazione dei principi privacy by design e by default e accountability previsti nel GDPR 679/2016 e in attuazione dell'art. 32 del citato Regolamento UE in particolare in particolare art.1 punto b) la capacità di assicurare su base

permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. Attraverso opportuni sistemi di comunicazione e formazione verranno fornite, in caso di variazione delle procedure, idonee istruzioni operative, che integreranno/sostituiranno quanto già indicato nelle lettere di autorizzazione al trattamento dati e a quanto previsto nel presente disciplinare tecnico.

Data la necessaria esiguità dello spazio a disposizione sul fileserver e l'erosione delle risorse di rete (ad es., connettività) che il riversamento di file comporta, è fatto divieto di salvare nelle cartelle materiale non direttamente attinente all'attività lavorativa.

SISTEMI ANTINTRUSIONE

Tutti i server, PC e notebook utilizzati dalla Istituto sono equipaggiati con specifico antivirus i cui aggiornamenti sono verificati e distribuiti centralmente attraverso specifiche politiche automatiche (aggiornamenti automatici).

Su ogni singola postazione di lavoro è inoltre installato un ulteriore sistema antimalware (se non incluso nell'antivirus anch'esso con aggiornamento automatico.

Tutti i sistemi di protezione indicati verranno configurati con funzioni di pianificazione di una scansione completa automatica su ogni dispositivo a cadenza periodica. Nel caso di impossibilità ad eseguire tale configurazione automatica, verranno fornite idonee istruzioni affinché ogni singolo utente possa eseguire autonomamente il Lancio della procedura di scansione completa sulla postazione di lavoro assegnata.

Tali strumenti si occupano quindi automaticamente sia della ricerca periodica dei files che consentono al motore antivirus di intercettare i codici maligni, sia dell'installazione che dell'aggiornamento automatico della protezione. Lo stato degli aggiornamenti e delle eventuali incidenze virali è monitorato centralmente da una o più postazioni di competenza degli amministratori di sistema.

Ove tecnicamente possibile in relazione all'attribuzione di account privilegiati, è fatto divieto di alterare, disabilitare o modificare tale programma.

Nel caso in cui il software antivirus rilevi la presenza di un virus, ovvero l'utente riscontri una anomalia che possa essere riconducibile all'aggressione di un agente dannoso (reindirizzamento di pagine web, messaggi indesiderati, blocco di programmi, rallentamenti, etc.), è fatto obbligo di segnalare immediatamente il problema all'Amministratore di Sistema e/o al Titolare.

Queste misure sono adotta in attuazione di quanto previsto nell'Analisi dei rischi in attuazione della normativa sulla privacy e di quanto previsto in attuazione di quanto previsto nelle misure di sicurezza minime AGID livelli M ed S.

UTILIZZO DELLE RISORSE DI SISTEMA

È vietato connettere autonomamente e senza autorizzazione dell'Ufficio Servizi Informatici e Tecnologici alla rete informatica/telefonica dell'Ente apparati di qualunque genere, inclusi Hub, Switch, Router, Access Point Wi-Fi, Modem, Computer Laptop, Computer Desktop, Print Server, Stampanti, Analizzatori di rete (Hardware e Software), apparati in genere dotati di interfaccia Ethernet. Tali operazioni vanno preventivamente comunicate all'Amministratore di Sistema e Tecnologici che ne valuterà l'effettiva necessità e la relativa fattibilità e, in caso di approvazione, si occuperà dell'attività di configurazione e messa in sicurezza dell'apparato in oggetto.

Gli utenti non devono abusare delle risorse informatiche e telematiche, alterandole o facendone cattivo uso attraverso:

- tentativi intenzionali di apportare modifiche a sistemi o altre risorse informatiche per cui l'utente non possieda idonea autorizzazione[8];
- modifiche di configurazioni di sistemi di uso collettivo;
- tentativi intenzionali di bloccare o mandare fuori servizio computer, reti, servizi od altre risorse;
- più in generale, attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti;
- danneggiamento o vandalismo nei confronti di apparati, software, files o altre risorse informatiche e/o telematiche.

Si fa presente che alcune delle indicate condotte costituiscono reati perseguibili ai sensi della legge n. 547/1993.

ARCHIVI INFORMATICI CONTENENTI DATI PARTICOLARI (EX "DATI SENSIBILI")

In relazione a specifiche funzioni (ad es., acquisti/risorse umane) o ad attività con altri Enti (ad es., quelle che comportino verifiche amministrative per conto di Titolari committenti sul possesso di determinati requisiti), è possibile che vengano acquisiti e detenuti **archivi (cartelle) contenenti dati sensibili e/o dati giudiziari**.

Queste cartelle/sottocartelle **non devono mai essere liberamente accessibili** ma protette secondo livelli di autenticazione limitati ai soli soggetti autorizzati. Per evitare che eventuali (improbabili ma sempre possibili) accessi abusivi dall'esterno possano compromettere la riservatezza di tale documentazione, **è necessario che tali archivi siano cifrati (in caso impossibilità di cifratura è necessario l'applicazione di ulteriori misure ad es., zippati con password e l'applicazione ove possibile della pseudonomizzazione) e, se detenuti in formato cartaceo, custoditi in contenitori chiusi a chiave ed accessibili solo ai soggetti autorizzati.**

L'implementazione di tali misure è sottoposta a verifiche periodiche.

INSTALLAZIONE DI SOFTWARE

Ove tecnicamente possibile in relazione all'attribuzione di account privilegiati:

- non è consentito installare autonomamente programmi (o file eseguibili)[9] provenienti dall'esterno (ad es., software scaricato da internet, contenuto in supporti allegati a riviste, libri e quotidiani, prestati da amici etc.);

[8] Ad es., rimuovere programmi software od apparati hardware.
[9] Sono file eseguibili, per es., i seguenti: .exe; .com; .bat; .cmd; .net.

- è assolutamente vietato installare, anche solo temporaneamente, programmi ottenuti o sbloccati illegalmente (programmi crackati, codici di sblocco ottenuti da internet, ecc.);
- è, inoltre, tassativamente proibito utilizzare la capacità di calcolo e l'infrastruttura di rete allo scopo di connettersi ad Internet nei circuiti/protocolli Peer2Peer e/o di filesharing (ad es., BitTorrent, FastTrack, etc.), ovvero per la generazione di moneta digitale (es.: bitcoin, etc.).

Se il proprio lavoro richiede l'utilizzo di programmi specifici è necessario consultare preventivamente l'Ufficio Servizi Informatici e Tecnologici che valuterà se consentire o meno l'operazione.

E' vietato effettuare copie non autorizzate e/o distribuire software soggetto a diritti di proprietà industriale o intellettuale (es.: diritto di autore) acquisito dall'Ente, al di fuori dei termini e dalle modalità previsti dalle relative licenze.

Per l'Applicazione e la verifica di tali visure è necessario la tenuta e l'aggiornamento del REGISTO dei SOFTWARE MISURE MINIME DI SICUREZZA AGID ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

UTILIZZO DI ULTERIORI DISPOSITIVI E STRUMENTI AZIENDALI

DISPOSIZIONI GENERALI

Per motivate esigenze di servizio, il personale dell'Ente può essere dotato di ulteriori dispositivi e strumenti aziendali da utilizzare per consentire l'attività e la connessione ai servizi informatici dell'Ente.

L'attività può essere svolta anche fuori sede e oltre l'orario di lavoro, nel rispetto delle disposizioni di seguito indicate.

Computer portatili

In funzione delle scelte organizzative, l'Ente può assegnare ai lavoratori – in alternativa ad un computer fisso, ovvero temporaneamente – un computer portatile.

L'utente è responsabile del dispositivo assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.

Ai computer portatili si applicano le regole di utilizzo previste per i computer fissi. **Per motivi di sicurezza, per chi utilizza computer portatili è obbligatorio lavorare solo su *file* archiviati nel *file* server, non salvando dunque i *file* di lavoro in locale sulla macchina**.

Tali regole trovano applicazione anche nel caso dei dispositivi consegnati ai dipendenti che svolgono attività di *smart working*. Questi, al termine della giornata di lavoro e prima di riconsegnare il dispositivo, curano la cancellazione di eventuali dati personali presenti sul dispositivo. Quanto detto vale anche nel caso in cui l'attività è articolata su un intervallo temporale più lungo.

I computer portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che si rendono necessari per evitare danni o sottrazioni.

Di norma, non è consentito l'utilizzo di supporti magnetici removibili per la memorizzazione di informazioni (es. dispositivi USB o hard disk esterni) salvo non sussistano comprovate esigenze d'ufficio che lo giustifichino e ferma restando la necessità di adottare idonee cautele al fine di prevenire la perdita o l'accesso non autorizzato ai dati (cifratura).

Stampanti

L'Istituto mette a disposizione dei propri lavoratori apposite macchine stampanti "di Rete" – anche con modalità c.d. multifunzione - che consentono varie operazioni tra cui la copia cartacea di documenti, la scansione e l'invio via mail degli stessi.

Non è consentito, se non occasionalmente ed in misura limitata, l'utilizzo delle stampanti aziendali per fini personali. L'istituto equipaggia tali dispositivi con tecnologie di autenticazione in modo che solo ed esclusivamente il personale autorizzato possa prelevare la documentazione prodotta, garantendo al contempo una maggiore sicurezza del processo e la riservatezza dei dati trattati.

Alcune postazioni possono essere dotate di una stampante dedicata che funziona come periferica locale del personal computer. Valgono, per queste stampanti, le stesse regole delle stampanti "di Rete".

Tablet

Per i Tablet valgono le medesime regole di sicurezza e custodia previste per i computer portatili.

Telefoni cellulari (smartphone)

L'Istituto, compatibilmente con le esigenze organizzative, può mettere a disposizione dei propri dipendenti dei telefoni cellulari di servizio, definendone le condizioni di utilizzo.

Per motivi di sicurezza, l'accesso a tali dispositivi deve essere subordinato alla digitazione di un codice personale (PIN).

Tali regole trovano applicazione anche nel caso dei dispositivi *smartphone* consegnati ai dipendenti che, eventualmente, dovessero svolgere attività di *smart working*. Questi, al termine della giornata di lavoro e prima di riconsegnare il dispositivo, curano la cancellazione di eventuali dati personali presenti sul dispositivo. Quanto detto vale anche nel caso in cui l'attività è articolata su un intervallo temporale più lungo. Per l'attività di cancellazione è possibile, se del caso, chiedere l'assistenza dell'Amministratore di Sistema.

Nonostante le cautele di cui sopra, ove siano inevitabilmente presenti sul dispositivo mobile dati ed informazioni considerate critiche dal dipendente, questi dovrà richiedere l'attivazione - se tecnicamente possibile - della possibilità di blocco del dispositivo e la cancellazione dati da remoto in caso di furto. Le cautele di cui al presente par. trovano applicazione anche nel caso di utilizzo dei servizi di posta elettronica aziendale sullo smartphone di proprietà del dipendente, ad esclusione del caso in cui si acceda mediante web mail.

Webcam

Per le lo svolgimento delle attività lavorative i dipendenti possono essere dotati di webcam (sia essa collocata sul computer fisso), ovvero venga adoperata quella in dotazione del computer portatile.

L'utilizzo della webcam, escluso il tempo di connessione ed il relativo "indirizzo" della medesima, **non prevede da parte dell'Istituto alcun controllo, né alcuna registrazione dei contenuti delle comunicazioni.**

È vietato l'utilizzo di webcam per comunicazioni private.

CUSTODIA E PROCEDURE IN CASO DI MALFUNZIONAMENTO, DANNEGGIAMENTO, SMARRIMENTO O FURTO

L'utilizzo - anche al di fuori dell'orario di lavoro – degli ulteriori dispositivi e strumenti aziendali deve essere inerente all'attività lavorativa.

Gli strumenti utilizzati all'esterno dell'Ente (convegni, riunioni, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

L'assegnatario del dispositivo è **responsabile del suo corretto utilizzo** dal momento della presa in consegna fino alla restituzione e/o revoca e dovrà porre ogni cura nella sua conservazione, per evitare danni, smarrimenti o sottrazioni dello stesso e dei dati ed informazioni ivi contenuti.

Per quanto riguarda:

a) i personal computer (siano essi fissi che portatili) non forniti dall'Istituto ed impiegati dal lavoratore in smart work, possono essere previamente verificati dall'Amministratore di Sistema, al fine di "configurarli" per le attività lavorative. Il lavoratore presterà le debite accortezze per evitare danni, smarrimenti o violazione dei dati trattati in occasione delle attività inerenti il lavoro. Non è consentito da parte dell'Istituto alcun controllo sui dati e le informazioni contenute in detti computer qualora questi riguardino le attività personali del dipendente.

Malfunzionamento e danneggiamento

Qualora si dovesse riscontrare un malfunzionamento o un danneggiamento di personal computer, loro periferiche, ovvero altri dispositivi dell'Istituto (quali quelli descritti in precedenza) il lavoratore interessato ne fa comunicazione al competente titolare.

Smarrimento o furto

Nel caso di smarrimento o sospetto furto di personal computer, loro periferiche, ovvero altri dispositivi aziendali (quali quelli descritti in precedenza), di proprietà dell'Istituto è necessaria la tempestiva comunicazione al Titolare che provvederà, ad esporre regolare denuncia presso le autorità competenti.

Le comunicazioni indicate devono specificare se, all'interno vi siano dati personali non cifrati al fine dell'avvio – se del caso – della procedura di *Data Breach – Notifica e comunicazione agli interessati*.

PROCEDURE IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO

Al termine del rapporto di lavoro, per qualsiasi motivo esso avvenga:

- personal computer, tablet, smartphone ed altri asset di proprietà dell'Istituto devono essere restituiti;
- l'utente non deve eliminare/alterare/danneggiare files/dati/informazioni di qualsiasi tipo presenti nelle risorse ICT dell'Istituto e, in particolare, dai supporti rimovibili in uso, eccezion fatta per i dati personali eventualmente presenti;
- il dipendente non deve conservare/copiare/trasferire files/dati/informazioni di qualsiasi tipo facenti parte del Patrimonio Informativo dell'Istituto all'esterno dello stesso o su dispositivi privati.

UTILIZZO DI INTERNET E DELLA POSTA ELETTRONICA

UTILIZZO DI INTERNET

La stessa infrastruttura nonché numerosi sistemi informativi utilizzati dall'Istituto (e quindi strumentali all'attività istituzionale di cui deve essere garantita la assoluta continuità) sono *web oriented*, quindi un eccessivo traffico internet non legato a motivi di lavoro può comportare disservizi / blocchi su sistemi critici.

Per questo, il servizio di navigazione su Internet a fini personali è occasionalmente tollerato esclusivamente solo nella misura in cui non interferisca con i propri doveri d'ufficio e purché **non comprometta l'utilizzo delle citate risorse e la sicurezza complessiva del patrimonio aziendale** (beni, strumenti, dati ed informazioni).

Questa soluzione non esime comunque il dipendente dall'utilizzo corretto della navigazione web.

E' fatto esplicito divieto ai dipendenti dell'Ente di fornire la password dell'eventuale sistema Wi-Fi (riservato ai dipendenti) a visitatori o collaboratori occasionali; a questi ultimi andrà comunicata esclusivamente la password di accesso alla rete wireless predisposta per i navigatori GUEST.

L'Istituto, infatti, ha provveduto ad operare una separazione delle reti per la didattica e l'amministrazione e implementato sistemi di bilanciamento delle risorse in base alle necessità di utilizzo gestite al livello centrale con opportuni software di configurazione; ciò per finalità di sicurezza e di efficienza.

UTILIZZO DELLA POSTA ELETTRONICA ISTITUZIONALE

L'Istituto ha un sistema misto di caselle di posta elettronica "istituzionali" (con dominio @istruzione.it), identificabili come segue:

a) indirizzi **individuali** (nome.cognome@istruzione.it), basati sull'identità personale del dipendente ed attribuibili di regola a personale dipendente/distaccato dell'Ente, con accesso esclusivo da parte del diretto interessato;
b) indirizzi di **struttura** (ad esempio, meccanografico@istruzione.it), con accesso condiviso tra più utenti della stessa Struttura organizzativa, individuati dal relativo responsabile; questi deve inoltre definire e condividere all'interno della struttura le regole di gestione della e-mail, in modo da garantire la continuità ed operatività del servizio e, contestualmente, i principi di stretta necessità e di non eccedenza nel trattamento dei dati.

La casella di posta istituzionale è uno strumento di lavoro. Gli utenti assegnatari delle caselle di posta istituzionale sono responsabili del corretto utilizzo della stessa.

L'utilizzo della posta elettronica aziendale per finalità personali è tollerato in quanto non comprometta la sicurezza complessiva del patrimonio aziendale.

È espressamente vietato:

- salvo diversa ed esplicita autorizzazione, utilizzare l'indirizzo istituzionale per finalità private, quali a puro titolo esemplificativo:
  - ✓ partecipazione a dibattiti, forum o mailing-list, newsletter ed altri servizi on-line non pertinenti all'attività lavorativa;
  - ✓ invio o ricezione di:
    - informazioni indesiderate o invasive (c.d. "spam"), pubblicità non istituzionale, manifesta o occulta e comunicazioni commerciali private;
    - materiale pornografico o simile, che violi la dignità e riservatezza di eventuali interessati, ovvero che violi diritti di proprietà intellettuale di terzi (ad es., copyright).
- utilizzare, per qualunque finalità – istituzionale o privata - un account di posta elettronica "apparentemente" intestato alla Istituto(ad es., nomedellascuolaprovincia@gmail.com), ad un servizio (ad es., acquisti.meccanografico@gmail.com), ovvero ad un altro dipendente (ad es., nomecognome.meccanografico@libero.it), che può indurre in errore altri utenti[10].

Nell'utilizzare anche a fini istituzionali l'email aziendale, bisogna fare attenzione ai messaggi ricevuti, ed in particolare:

- in caso di dubbio sul mittente o sul contenuto (allegati sospetti) occorre controllare che non contengano virus o altri

codici malevoli: salvare l'allegato ed effettuare lo "scan" con il software antivirus PRIMA di aprire il file;

- la posta elettronica non desiderata (*spam*) o di cui non si conosce il mittente non deve essere aperta e va prontamente cancellata. Non bisogna mai rispondere a tali mail poiché si potrebbe incorrere nel rischio di aprire un varco a potenziali pericoli (virus, worm, trojan, etc.), ovvero semplicemente confermare l'esistenza dell'email ai fini dell'inserimento nelle liste di spam;
- bisogna cestinare – a meno che il mittente non sia "sicuro" – le email che invitino a cogliere una nuova "opportunità di lavoro", a dare le coordinate bancarie del proprio conto online o altri dati personali per verificarne l'attendibilità o l'esattezza, etc.[11].

Per quanto riguarda la posta elettronica in uscita:

- bisogna fare estrema attenzione all'indirizzo email digitato, per non compromettere la confidenzialità dei contenuti[12], nonché alla correttezza dell'allegato;
- qualora sia adottato un sistema di classificazione dei documenti interno dell'Istituto[13], non bisogna mai inviare tramite posta elettronica quelli classificati come *confidenziali*, *riservati*, *esclusivi,* a meno che non si riferiscano allo stesso soggetto mittente;
- se possibile, è sempre consigliabile utilizzare il comando Bcc[14] per inviare un messaggio a più soggetti, a meno che i singoli destinatari debbano sapere esattamente a chi è destinato il messaggio;
- nel caso in cui sia necessario inviare documenti contenenti dati particolari (sensibili/giudiziari), questi devono essere cifrati (ad es., zippati con password) e la relativa password di apertura deve essere comunicata al destinatario con un diverso canale di comunicazione (ad es., telefono/sms).

CONTINUITÀ DELLE COMUNICAZIONI

E' vietato configurare il servizio di posta elettronica aziendale su dispositivi (aziendali o personali) quali telefoni cellulari o tablet. Si richiama l'attenzione sulla necessità di impostare quantomeno un PIN all'accensione del tablet o del cellulare edi non salvare le password di accesso ad applicativi in cloud onde evitare in caso di smarrimento o furto e nei limiti delle misure disponibili sull'apparecchio, la possibilità di accesso ai dati ed informazioni ivi detenuti.

[10] Tale condotta può configurare fattispecie di reato quali quelle previste dagli artt. 494 c.p. (sostituzione di persona: "chiunque … induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o un falso stato…") e 640 c.p. (truffa: "chiunque, con artifizi o raggiri, indicendo taluno in errore …").

[11] Si tratta del fenomeno conosciuto come *phishing* (letteralmente "spillaggio" di dati sensibili): attività che, sfruttando una tecnica di ingegneria sociale, è utilizzata per ottenere illecitamente l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggiistantanei

[12] Tale condotta, pur non potendo configurare – in assenza di dolo specifico - un trattamento illecito di dati personali per comunicazione/diffusione a soggetti non autorizzati ai sensi dell'art. 167 del Codice, può dar luogo al risarcimento del danno eventualmente richiesto dal soggetto che ritenga lesa la sua dignità/riservatezza.

[13] Ad es., connesso alla classificazione della corrispondenza come riservata, personale etc.

[14] CCN = Copia Conoscenza Nascosta; BCC = Blind Carbon Copy.

POSTA ELETTRONICA PERSONALE

L'utilizzo di posta elettronica personale del dipendente, mediante accesso a servizi di web mail è consentito solo nella misura in cui non interferisca con i propri doveri d'ufficio e purché non comprometta l'utilizzo delle risorse e la sicurezza complessiva del patrimonio aziendale (beni, strumenti, dati ed informazioni).

E' comunque espressamente vietato configurare il software client di posta[16] installato su postazioni di lavoro dell'Istituto per la gestione di servizi di posta elettronica privata.

CANCELLAZIONE, RIASSEGNAZIONE E SMALTIMENTO DEI SUPPORTI DI MEMORIZZAZIONE

I supporti contenenti dati personali (soprattutto se particolari/giudiziari) devono essere smaltiti in modo da evitare il recupero di informazioni riservate, come previsto dal Garante[17].

La dismissione o formattazione per eventuale riassegnazione ad altro utilizzatore di tali supporti deve essere effettuata esclusivamente con una delle seguenti procedure:

a) specifici programmi informatici (quali *wiping program o file shredder*) che provvedono, una volta che l'utente abbia eliminato dei *file* da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati;
b) formattazione "a basso livello" dei dispositivi di tipo *hard disk* (*low-level formatting–LLF*), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
c) demagnetizzazione (*degaussing*) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, *floppy-disk*, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione *software*;
d) sistemi di punzonatura o deformazione meccanica, ovvero distruzione fisica o disintegrazione (usata per i supporti ottici come i cd-rom e i dvd).

[15] Attivando autonomamente le apposite funzionalità previste da web mail ovvero richiedendo il supporto dell'Ufficio Servizi Informatici e Tecnologici
[16] Ad es., Outlook, Thunderbird, Eudora, etc.
[17] Provvedimento del Garante 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali"

SISTEMA DI MONITORAGGIO E AUDIT

L'attività di verifica/monitoraggio sull'osservanza dei contenuti del presente Disciplinare per tutti gli aspetti relativi alla tutela dei dati personali è una competenza del titolare, controllata dal Responsabile della Protezione dei Dati (RPD).

Inoltre, il datore di lavoro, può riservarsi di verificare, anche tramite delegati espressamente autorizzati, se il prestatore utilizza la prescritta diligenza e osserva le disposizioni impartitegli, anche al fine dell'eventuale esercizio del potere disciplinare.

Nell'esercizio di tale prerogativa il datore di lavoro garantisce il **rispetto della libertà e della dignità dei lavoratori**, in particolare per ciò che attiene alla installazione ed utilizzo di "strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" (art. 4, comma 1, Statuto dei Lavoratori[18]).

Si rammenta che tali tutele non sono riferibili a fatti estranei alla prestazione lavorativa che presentino ad es., profili di illiceità od una aggressione a un bene oggetto di tutela di titolarità dell'azienda: **se il controllo tecnologico non è "preventivo" né "sistematico" ma "reattivo", ovvero finalizzato ad accertare condotte illecite del lavoratore**, può essere legittimamente utilizzato nel rispetto dello Statuto dei lavoratori[19].

L'Ente può avvalersi delle prerogative sopra menzionate per l'attuazione di un sistema di controllo e monitoraggio avente le seguenti finalità:

a) Controlli di routine

- audit finalizzati all'applicazione della normativa in materia di privacy e delle misure di sicurezza, comprese le istruzioni impartite dal Titolare attraverso il presente Disciplinare;
- verifiche annuali sugli amministratori di sistema, come previsto dal provvedimento del Garante citato in premessa.

b) Controlli occasionali o per specifiche finalità

- verifiche a campione sulla funzionalità e sicurezza di strumenti, apparati, e sistemi[20];
- verifiche ed indagini mirate a seguito di anomalie ed incidenti di sicurezza[21], per finalità di legge (ad es., gestione dei data breach ai sensi degli artt. 33 e 34 GDPR e secondo specifica procedura approvata) ovvero per finalità difensive[22];
- controlli in occasione di attività di manutenzione di dati e sistemi[23] e per necessità collegate alla sicurezza sul lavoro;
- controlli e verifiche effettuate sulla base di specifica richiesta dell'autorità inquirente o della polizia giudiziaria.

In ogni caso, è esclusa l'effettuazione di controlli prolungati, costanti ed indiscriminati, con finalità di controllo a distanza dell'esatto adempimento delle obbligazioni derivanti dal rapporto di lavoro (c.d. "non lavoro" o "tempo/macchina").

VERIFICHE SU LOG E POSTA ELETTRONICA

VERIFICHE SUI LOG

Log di sistema

[18] Come modificato dall'art. 23 del D.Lgs. 14 settembre 2015, n. 151.
[19] In proposito, ad es., Cass., sez. lav., 23 febbraio 2012, n. 2722.
[20] Ad es., controlli a campione sulle impostazioni degli applicativi atti a prevenire l'incidenza di codici maligni (c.d. antivirus); controlli a campione sugli spazi di backup assegnati agli utenti, al fine di verificare che l'eventuale salvataggio di file non relativi alle normali attività lavorative non causi blocchi o malfunzionamenti al sistema ovvero non configuri ipotesi di reato; salvataggio di file di cui l'operatore non detiene i diritti di utilizzazione (file audio e video scaricati dalla rete, programmi ottenuti o sbloccati illegalmente), file corrotti da virus/spyware in grado di compromettere l'intera infrastruttura informatica, etc.
[21] Ad es., incidenza di virus, commissione di illeciti, accessi abusivi a sistemi e dati, etc.
[22] ovvero forme di intervento, controllo o monitoraggio diretti ad accertare condotte illecite del lavoratore che integrino, appunto, lesione del patrimonio dell'Ente ovvero delle vere e proprie fattispecie di reato, al fine di far valere il proprio diritto in sede giudiziaria.
[23] con l'obbligo dei soggetti incaricati della manutenzione - formalizzato con apposite lettere d'incarico - di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità.

Alcuni strumenti di elaborazione (ad es.: sistemi operativi, specifici software gestionali) implementano sistemi di memorizzazione di alcune informazioni relative all'accesso ed all'utilizzo degli stessi (c.d. file di log). Le informazioni gestite sono del tipo *access log*, ovvero registrazione degli eventi (*event records*) generati dal sistema di autenticazione informatica: contengono usualmente i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*), una descrizione dell'evento (sistema di elaborazione o software utilizzato, se si tratti di un evento di *log-in*, ovvero di *log- out*).
La registrazione e conservazione di tali informazioni per periodi di tempo limitati è conforme all'attuale previsione dell'art. 4, comma 2 dello Statuto dei Lavoratori.

In proposito si specifica che:

- con **riferimento alla generalità dei dipendenti dell'Istituto, non sono installati né utilizzati specifici software per il monitoraggio delle attività informatiche ma possono essere utilizzati quelli resi disponibili dai sistemi in uso;**
- esclusivamente nel caso delle utenze di **amministratore di sistema**, l'Istituto potrà dotarsi di uno specifico **sistema di log management** che ne garantisca il monitoraggio con caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Si specifica che in questo caso, l'adempimento è richiesto specificamente dal provvedimento del Garante del 27 novembre 2008 in materia di "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" citato in premessa, per finalità di verifica della rispondenza del loro operato alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti ed impartite dal Titolare del trattamento.

Infine si ribadisce che **non sono in alcun modo utilizzati** sistemi per:

- ✓ la lettura e la registrazione dei dati sull'attività interattiva (ad es., caratteri inseriti tramite la tastiera o analogo dispositivo);
- ✓ l'analisi occulta di computer affidati in uso;
- ✓ Sistemi MDM (Mobile Device Management) per la geolocalizzazione dei dispositivi aziendali.

Log di navigazione

L'Istituto attualmente **non implementa soluzioni per il tracciamento e l'elaborazione della navigazione Internet.**

I *log* registrati dal firewall sono accessibili esclusivamente da Amministratori di sistema, specificamente nominati, che dispongono dei permessi necessari per accedere a tali dati. Gli accessi degli Amministratori di sistema sono tracciati.

I *log*, inoltre, sono trattati in maniera tale da fornire informazioni aggregate, così da precludere l'immediata identificazione degli utenti, salve le richieste di accesso puntuali che vengano formulate dalle Autorità Giudiziarie competenti.
Eventuali controlli sui *log* possono essere svolti esclusivamente nei limiti di cui al paragrafo *Controlli e sanzioni*.

Conservazione dei dati di log

E' prevista la cancellazione periodica (attraverso procedure di sovra registrazione come, ad esempio, la c.d. rotazione dei log file) dei record la cui conservazione non sia necessaria o richiesta da specifiche disposizioni legislative[24], a cura dell'amministratore di sistema.

Può essere disposta la conservazione oltre i limiti previsti dalla legge **esclusivamente** nei casi in cui ciò sia necessario per:

1) l'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
2) ottemperare ad una specifica richiesta da parte delle pubbliche autorità (magistrato o forze dell'ordine con funzioni di polizia giudiziaria);
3) ottemperare al Provvedimento del Garante relativo alle attività degli amministratori di sistema.

[24] Per gli operatori telefonici e gli ISP (Internet Service Provider), si v., ad esempio, l'art. 24, della legge n. 167/2017.

ACCESSO ALLE EMAIL ISTITUZIONALI

Non è possibile per l'Istituto effettuare l'accesso diretto alla casella di posta elettronica istituzionale dei dipendenti.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, l'Istituto svolge attività di informazione e formazione con riferimento ai contenuti del presente Disciplinare.

CONTROLLI E SANZIONI

MODALITA' DEI CONTROLLI

L'Istituto si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli saltuari e a campione che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni.

I controlli sono effettuati dall'Amministratore di sistema su richiesta del Titolare del trattamento dati.

I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti su dati aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifici audit informatici.

A seguito di detto controllo anonimo, laddove fosse rilevata una effettiva e grave anomalia dell'attività, potrà essere emesso un avviso generalizzato, con l'invito ad attenersi esclusivamente e scrupolosamente ai compiti assegnati ed alle istruzioni impartite.

Se a detta comunicazione non dovessero seguire, nei quindici giorni successivi, ulteriori anomalie, l'Istituto non procederà a ulteriori controlli.

In caso contrario, verranno inoltrati preventivi avvisi, sempre su base anonima, riferiti all'unità organizzativa dalla quale provenga l'anomalia riscontrata.

Qualora continuino i comportamenti sono effettuati controlli nominativi o su singoli dispositivi e postazioni e, a seconda della gravità della violazione riscontrata, saranno applicate le sanzioni di cui al paragrafo successivo.

In ogni caso non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati.

L'Istituto inoltre non effettuerà, in nessun caso, né farà effettuare da eventuali Responsabili esterni, trattamenti di dati personali mediante sistemi *hardware* e/o *software* che mirino al controllo a distanza dei lavoratori, ovvero a ricostruire l'attività del lavoratore, quali a titolo esemplificativo e non esaustivo:

- lettura e/o registrazione sistematica dei messaggi di posta elettronica, ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio di posta elettronica stesso;
- riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore, dei contenuti delle medesime, nonché del tempo di permanenza sulle stesse;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di computer o altri dispositivi portatili affidati in uso, ovvero delle rispettive connessioni ad Internet.

Resta sempre salvo l'obbligo dell'Istituto di comunicare i *log file* contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle Autorità Giudiziarie competenti che ne facciano richiesta secondo la normativa vigente.

SANZIONI

È fatto obbligo a tutti i dipendenti/collaboratori interessati di osservare le disposizioni del presente Disciplinare.

Il mancato rispetto o la violazione delle regole sopra descritte è perseguibile nei confronti del personale dipendente o equiparato con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

Per il personale non dipendente troveranno applicazione le sanzioni previste nei contratti che disciplinano la loro attività, ferma restando l'applicazione di tutte le azioni civili e penali consentite.

L'Istituto, nell'esercizio della facoltà di verificare l'esatto adempimento della prestazione professionale ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti/collaboratori, salvaguarda in ogni caso la libertà e la dignità, attenendosi scrupolosamente ai limiti previsti dalla normativa.

DISPOSIZIONI FINALI

INTERPRETAZIONE, MODIFICHE E DEROGHE

Interpretazione

Per qualsiasi questione inerente gli aspetti tecnico-informatici di cui al presente disciplinare è possibile rivolgersi all'Amministratore di Sistema.
Le questioni inerenti la tutela dei dati personali sono di competenza dell'RPD dell'Ente.

Modifiche e deroghe

Le modifiche al presente Disciplinare sono disposte con provvedimento adottato con la stessa procedura seguita per la sua approvazione.
Eventuali comportamenti non rispondenti con quanto previsto dal presente Disciplinare, che venissero comunque tollerati dall'Istituto, non costituiscono una rinuncia dello stesso ad esercitare successivamente i suoi diritti per far valere le prescrizioni del Disciplinare.

IL DIRIGENTE SCOLASTICO
Claudia SCIPIONI
Documento firmato digitalmente ai sensi del
Codice dell'Amministrazione digitale e norme ad esso connesse