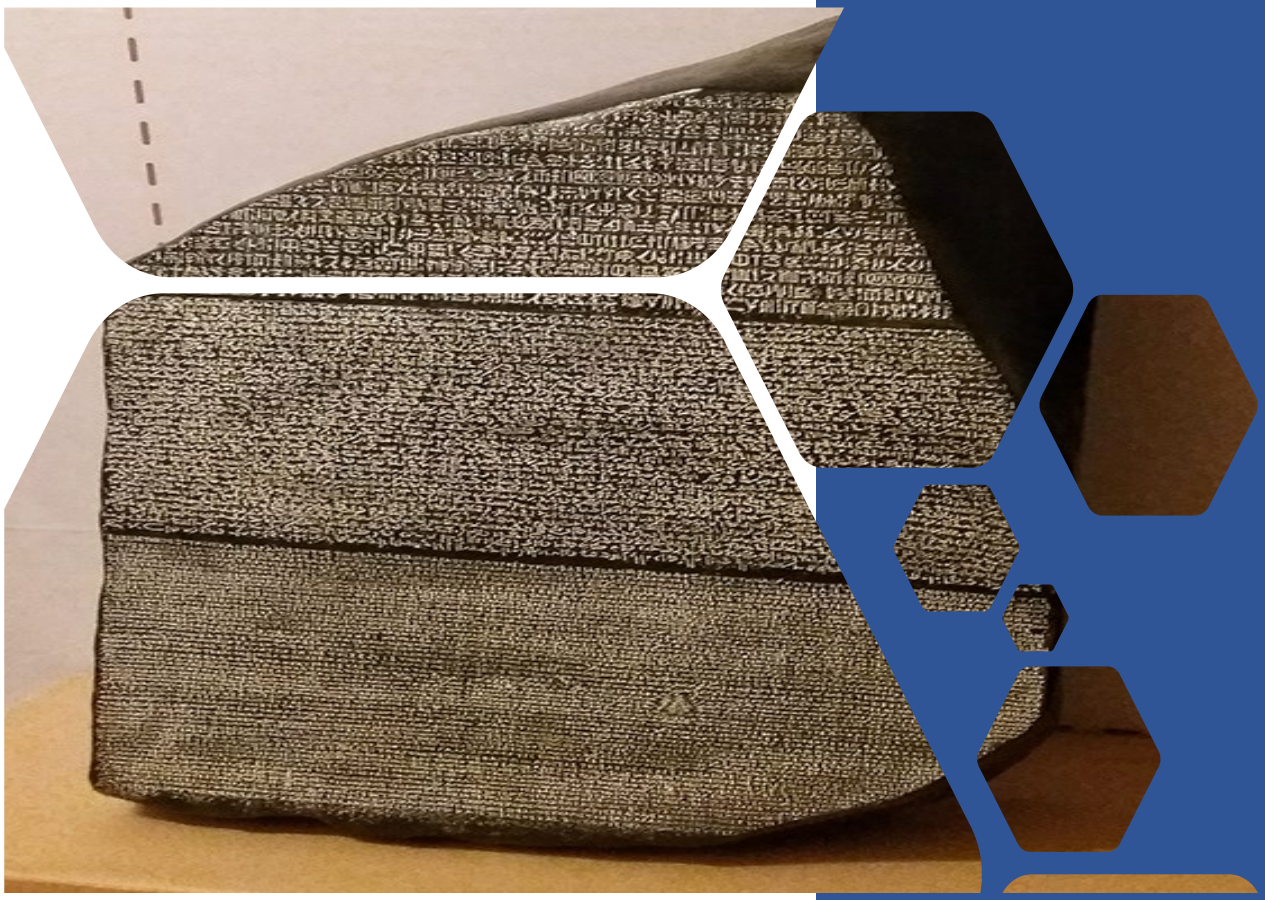
REGOLAMENTO IT AZIENDALE



Sommario

CAPO I - Disposizioni generali

Art. 1. - Ambito di applicazione - Perimetro

1) Il presente Regolamento si applica a tutti gli utilizzatori dei sistemi e dei servizi IT dell'organizzazione compresi nel perimetro, corrispondente alla massima estensione della rete di comunicazione privata fino al firewall di connessione con la rete pubblica, includendo anche i sistemi collegati via Virtual Private Network (VPN) e i sistemi posizionati in zone demilitarizzate (DMZ), in *colocation*, in *hosting*, in *housing* o in cloud.
2) Sono compresi tutti gli elementi della catena tecnologica come le *facility*, il network, i sistemi server, il *middleware*, le applicazioni come anche i sistemi di gestione della sicurezza, il monitoraggio e il controllo, i dispositivi client come i personal computer, i *thin client*, le stampanti multifunzione, i centralini telefonici, i telefoni basati su tecnologia IP, gli smartphone e i tablet.
3) Sono escluse dal perimetro tutte le reti Wi-Fi di tipo *guest* (ad accesso gratuito per il pubblico).
4) Gli utilizzatori dei servizi pubblicati e accessibili da Internet sono esclusi dal perimetro se collegati attraverso connessioni esterne al perimetro (ad esempio sono esclusi coloro che visitano i siti web istituzionali, la sezione relativa agli obblighi di amministrazione trasparente, la consultazione dei referti e degli esami diagnostici online).

Art. 2. - Applicazione del Regolamento IT

1) Gli utenti sono obbligati ad accettare e a conformarsi al presente Regolamento come condizione necessaria per l'accesso e l'utilizzo dei servizi e dei sistemi IT.
2) Il rispetto delle prescrizioni è il prerequisito per un impiego legittimo e ottimale dei servizi e dei sistemi IT, sia per il personale deputato alla gestione che per tutti gli utilizzatori.

Art. 3. - Definizioni

Ai fini del presente regolamento s'intende per:

1) **Minaccia**: qualcosa di potenzialmente pericoloso; possibile evento non desiderato che porta alla perdita di riservatezza, integrità o disponibilità delle informazioni;
2) **Vulnerabilità**: caratteristica dei sistemi e dei processi che identifica una fragilità, un punto debole che in particolari condizioni, può comportare la perdita di riservatezza, integrità o disponibilità delle informazioni;
3) **Contromisure:** azioni di prevenzione e mitigazione delle vulnerabilità individuate al fine di limitare i rischi di perdita di riservatezza, integrità o disponibilità delle informazioni;
4) **Rischio:** probabilità che un evento si verifichi ovvero che una minaccia si trasformi in evento indesiderato e dannoso sfruttando una vulnerabilità;
5) **Fonte di rischio:** elemento tangibile o intangibile che possiede il potenziale intrinseco di originare il rischio singolarmente o in combinazione con altri elementi;
6) **Evento sfavorevole:** particolare insieme di circostanze in grado di modificare in modo negativo e contrario rispetto al normale comportamento di un sistema, ambiente, processo, flusso di lavoro o di una persona;
7) **Conseguenza:** Effetto diretto o indiretto di un evento;
8) **Incidente alla sicurezza:** Evento volontario o involontario attribuibile a una o più persone con associato un costo economico diretto (es. sostituzione del bene e interruzione del servizio) oppure indiretto (uso non autorizzato di informazioni, violazioni di legge, danni di immagine e reputazionali) che comporta una minaccia alla sicurezza;
9) **Impatto (negativo):** Stima delle potenziali perdite dirette o indirette associate a un rischio;

10) **Credenziali di autenticazione:** codice per l'identificazione dell'utilizzatore di un sistema o di un dispositivo associato a una parola chiave riservata, conosciuta solamente dal soggetto (spesso identificata come coppia login o codice utente e password) e che lo identificano univocamente;
11) **Spam:** ovvero spazzatura spesso associata alla posta elettronica (in inglese *junk e-mail*) che indica la ricezione di messaggi spesso indesiderati, ripetuti o monotematici (es. pubblicità) il cui mittente speso è sconosciuto.

Art. 4. - Principi

1) I principi ispiratori del presente regolamento sono:
   a) Tutela dei diritti, delle libertà e della dignità delle persone;
   b) Garanzia della necessaria *continuità operativa* per la miglior cura possibile dei pazienti e il minor dispendio di energie (umane, tecnologiche, temporali ed economiche);
   c) Tutela del patrimonio informativo dell'organizzazione e riduzione dei rischi connessi al trattamento dei dati e quindi della probabilità di:
      i. Accessi illegittimi ai sistemi o agli applicativi;
      ii. Modifiche indesiderate alle informazioni;
      iii. Perdita della disponibilità dei dati;
   d) Conformità normativa e allineamento agli standard di mercato;
   e) Riduzione della superficie di esposizione rispetto alle vulnerabilità ovvero le debolezze sistemiche trasformabili in un evento indesiderato nel caso si attui una minaccia;
   f) Corretto bilanciamento tra usabilità e sicurezza, adottando contromisure basate sull'Analisi dei rischi;
   g) Adozione della Regola del minimo previlegio rispetto alla finalità (*separation of duties policy*), in ottica di stratificazione dei profili e degli accessi;
   h) Diritto alla disconnessione degli utilizzatori dai sistemi *mobile* al di fuori dell'orario di lavoro.

Art. 5. - Condotta e utilizzo etico dei servizi e dei sistemi IT

2) I sistemi e i servizi IT sono forniti agli utenti per condurre e supportare la missione dell'organizzazione, ovvero tutte le attività legate agli ambiti tecnici ed amministrativi.
3) Gli utenti sono responsabili dell'utilizzo dei sistemi e dei servizi IT in modo eticamente corretto, sicuro, legale e conforme al presente regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'organizzazione.
4) L'utilizzatore di sistemi e servizi IT è direttamente responsabile di tutte le attività effettuate con gli account dell'organizzazione ricevuti, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel proprio personal computer, applicativo software o piattaforma web dell'organizzazione scolastica e non.
5) All'utilizzatore di sistemi e servizi IT sono tassativamente vietate le seguenti attività:
   a. La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;
   b. La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;
   c. La trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri o non omologati dai Sistemi Informativi Dell'organizzazione;
   d. L'invio di dati di tipo sensibili, tra cui documenti e dati personali, su canali non sicuri (esempi di strumenti da evitare per inviare dati sensibili sono whatsapp e la posta elettronica dell'organizzazione, che viaggia in chiaro quando inviata ad altro dominio di posta); è da ritenersi invece accettabilmente sicuro l'invio ad altro utente di posta dello stesso dominio.

In caso di dubbi è necessario contattare i Sistemi Informativi Dell'organizzazione o adottare tecniche di criptazione con invio della chiave su altro media);

e. La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'organizzazione;
f. L'accesso non autorizzato ai sistemi o ai servizi IT.

6) Gli utilizzatori di sistemi e servizi IT non sono autorizzati a rispondere a interviste telefoniche o sondaggi, compilare questionari on-line (anche se sollecitati da importanti *brand*).
7) L'introduzione degli strumenti mobili (forniti dall'organizzazione o BYOD) pone il problema dell'equilibrio tra vita privata e vita professionale, data la progressiva trasformazione degli strumenti di comunicazione da asincroni a tempo reale. È riconosciuto all'utilizzatore il diritto alla disconnessione[1] dai dispositivi *mobile* al di fuori dell'orario di lavoro e dai turni di pronta disponibilità.
8) Anche nel caso dei sistemi di *instant messaging* (es. WhatsApp) vale il diritto alla disconnessione; è demandato alla sensibilità dei singoli il rispetto della distinzione tra tempistiche professionali e momenti da dedicare alla vita privata e familiare.

CAPO II - Strumenti

Art. 6. - Identificazione, autenticazione e autorizzazione

1) L'organizzazione implementa nella gestione dei sistemi e dei servizi IT, la famiglia di protocolli AAA basata sulle funzioni di Autenticazione, Autorizzazione, Accounting (v. articolo successivo).
2) L'accesso alla rete e ai sistemi dell'organizzazione è possibile soltanto se l'utilizzatore:
   a) È stato prima di tutto ***identificato*** ovvero sono conosciute le sue generalità ed è stato dotato di credenziali utente (nome utente, password e/o PIN), soggette alle condizioni previste in questa sezione del Regolamento;
   b) Effettua l'***autenticazione*** tramite immissione delle credenziali, in modo che il sistema possa verificare se l'individuo è chi sostiene di essere, permettendone univoca identificazione;
   c) È stato ***autorizzato*** ovvero è stato conferito il diritto ad accedere a specifiche risorse in base al ruolo ricoperto, al profilo e alle specifiche mansioni assegnate.
3) La responsabilità delle azioni effettuate utilizzando la coppia "nome utente e password e/o PIN" sarà attribuita in termini di responsabilità al soggetto titolare dell'account, a meno di comprovato illecito da parte di terzi. Sono escluse le attività di supporto autorizzate dagli stessi utilizzatori per interventi di manutenzione o assistenza tecnica.
4) **Gli account di accesso del personale dipendente, dei consulenti esterni e dei fornitori sono di tipo nominativo e non riutilizzabile da altri soggetti, anche dopo la conclusione del rapporto di lavoro.**
5) Gli account di accesso hanno, per impostazione predefinita, una scadenza corrispondente alla data di fine del contratto, convenzione o accordo. È a carico dell'Istituto Scolastico comunicare al personale dei Sistemi Informativi l'eventuale prolungamento del contratto e la necessità di estensione temporale delle autorizzazioni (attività obbligatoria nel caso di mancata copertura da parte del sistema di gestione dell'organizzazione delle identità, direttamente integrato con il gestionale HR).

[1] L'articolo L. 2242-8 del Codice del lavoro francese ("*Code du travail*") modificato dalla legge Loi n° 2016-1088 (*relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels)* dispone "Le modalità di esercizio da parte del dipendente del proprio diritto alla disconnessione nonché la messa a disposizione di dispositivi che regolano l'utilizzo degli strumenti informatici, al fine di assicurare il rispetto dei tempi di riposo, del periodo di ferie e della vita personale e familiare". In Italia esiste al momento solo un disegno di legge n. 2233 su lavoro autonomo.

6) Il personale dei Sistemi Informativi specificatamente autorizzato gestisce gli account utente per tutto il ciclo di vita tramite apposita procedura (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, disattivazione una volta concluso il rapporto di lavoro).
7) La normativa vigente in tema di protezione dei dati, le norme volontarie e le *best practice* di settore impongono di stratificare le possibilità di accesso ai sistemi e ai servizi IT al fine di garantire un adeguato livello di sicurezza. Ad ogni account utente è collegato uno specifico *profilo di autorizzazione* che permette al singolo utilizzatore l'accesso in funzione del proprio ruolo, delle attività a cui è delegato e specificatamente autorizzato da un superiore (o soggetto Designato ai sensi del D.lgs. 196/03 e ss.mm.ii.). Le eventuali estensioni o eccezioni devono essere autorizzate e tracciate secondo procedura.
8) Il sistema di Autenticazione, Autorizzazione e Registrazione degli accessi ha l'obiettivo di garantire un adeguato livello di sicurezza, conforme a quanto previsto dalla normativa vigente e dal presente regolamento, poiché traccia, separa gli accessi nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni trattate.
9) La politica di sicurezza dell'organizzazione prevede la necessità di accesso ai sistemi tramite autenticazione a più fattori (MFA) tramite le modalità multiple previste dai sistemi (QR-Code, PIN, OTP temporaneo).

Art. 7. - Registrazione delle attività (*Accounting*)

1) A partire dall'accesso ai sistemi o ai dispositivi, le attività degli utilizzatori sono registrate in appositi file detti di *log*. Nei sistemi critici, di particolare rilevanza o di fede privilegiata sono memorizzate tutte le singole attività svolte riportando account utente, indirizzo o nome macchina, ora, data e il dettaglio delle azioni svolte, incluso il protocollo utilizzato.
2) Al fine di contenere lo spazio necessario alla conservazione, i file di log sono conservati in logica di rotazione, ovvero sono sovrascritti al raggiungimento di una certa data o di una certa dimensione.
3) Alcuni file di log (es. log di accesso) sono conservati nei sistemi per almeno 2 anni dall'evento.

Art. 8. - Corretto uso delle Credenziali di autenticazione

1) Le credenziali di autenticazione sono composte da un codice (account utente) facilmente riconducibile al soggetto e da una *password e/o PIN conosciuti al solo utilizzatore*. ***È tassativamente vietato rivelare la propria password*** di accesso alla rete, agli applicativi o servizi disponibili (inclusi i siti regionali o ministeriali), anche a terzi autorizzati. Qualsiasi azione effettuata utilizzando la coppia "account utente e password e/o PIN" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.
2) La *lunghezza minima della password* deve essere di almeno 14 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri[2] per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e per gli account qualificati amministrazione di sistema.
3) Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione (es. Mi_P1@c3_l4_P1zz@).
4) È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. L'eventuale violazione di un sistema potrebbe comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, dell'organizzazione e personali, riconducibili allo stesso soggetto.
5) Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 3 mesi (cd. *Password aging*).

[2] Misura minima prevista da AgID - «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017)

6) Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, oppure essere troppo ovvie (es. 'P@ssword').
7) Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (il precedente elenco non è esaustivo).
8) Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (criteri di complessità).
9) Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. *Password history*);
10) Le password degli account di accesso ai sistemi non sottoposti alle politiche di complessità, di invecchiamento o di rotazione impostate nel sistema di autenticazione centrale, devono comunque rispettare le medesime regole, agendo manualmente.
11) Le password e i PIN non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso o primo invio). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.
12) La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti.
13) I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.
14) È vietata la memorizzazione delle password nei browser o tramite applicativi di gestione password (es. Pocket Password) se non direttamente autorizzati/distribuiti dai Sistemi Informativi (nel caso si utilizzi Mozilla Firefox è possibile memorizzare le password nel browser solo nel caso di attivazione della funzione 'Utilizza una password principale' inserendo una password estremamente complessa e lunga). Sono comunque esclusi sistemi o applicativi software di memorizzazione delle credenziali nel cloud.
15) Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile al solo fine di verificarne la robustezza; es. https://password.kaspersky.com/it).
16) Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).
17) Non seguire le mode del momento, utilizzare acronimi, pattern ('CristianoRonaldo$' oppure sempre il primo carattere di ogni parola maiuscolo e un dollaro finale), ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari (in
18) *Appendice 1 - Password presenti nei dizionari* pubblici sono riportate degli esempi di password da NON utilizzare).
19) Nel caso di perdita (o anche solo il sospetto di perdita) della segretezza della password è necessario:
    a. Modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e Cambia password; verificare le modalità per i singoli applicativi software con autenticazione locale);
    b. Comunicare l'accaduto ai Sistemi Informativi dell'organizzazione, al proprio Responsabile e al DPO per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure del caso.
20) Nel caso l'utilizzatore sbagli per più di 5 volte l'inserimento della password, l'account è automaticamente disabilitato; per effettuare la riabilitazione dell'account è necessario contattare il supporto tecnico, aprire un ticket o, se presente, utilizzare il sistema di *self-service password*.

21) In caso di prolungato inutilizzo dell'account (per più di 6 mesi), in caso di cessazione o trasferimento degli utilizzatori, il sistema di Gestione delle Identità provvede all'automatica disabilitazione. L'eventuale riabilitazione dovrà essere autorizzata da un superiore, cosiddetto soggetto Designato.
22) Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, i Sistemi Informativi sono autorizzati alla momentanea disattivazione dell'account e del sistema utilizzato. Risolta la problematica evidenziata sarà cura dei Sistemi Informativi ripristinare le precedenti autorizzazioni.
23) Le richieste di cambiamento o reset password dell'account di accesso ai sistemi dell'organizzazione non sono mai inviate tramite e-mail. Eventuali e-mail che richiedano tramite link la modifica della password devono essere marcate come spam e cestinate.
24) È tassativamente vietato memorizzare account di accesso ai sistemi e servizi dell'organizzazione in documenti salvati in sistemi o dispositivi al di fuori del perimetro dell'organizzazione e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive o Dropbox).
25) Gli account di amministrazione di dominio possono essere utilizzati soltanto nei client assegnati al personale dei Sistemi Informativi o posizionati nel data center; questo al fine di evitare problemi di registrazione delle password attraverso *keylogger* hardware o software.

Art. 9. - Posta elettronica convenzionale

1) La posta elettronica è uno strumento di comunicazione e deve essere utilizzato soltanto per effettuare corrispondenze legate al servizio svolto nell'organizzazione.
2) Ogni utilizzo della posta elettronica deve essere effettuato coerentemente con le politiche e le procedure dell'organizzazione nel rispetto dell'etica, della sicurezza e in piena conformità alle leggi applicabili.
3) L'utilizzatore è tenuto a controllare almeno una volta a giorno il proprio account di posta elettronica per verificare l'eventuale arrivo di nuovi messaggi e conseguentemente l'assegnazione di specifici compiti.
4) La posta elettronica è erogata esclusivamente in modalità web, con accesso tramite browser. Sono tassativamente escluse altre modalità considerate non sicure come client locali di posta elettronica (es. Outlook o Mozilla Thunderbird) sia sui personal computer che sui dispositivi mobili, tablet o smartphone personali (BYOD). Eventuali deroghe dovranno essere autorizzate dal Dirigente Scolastico.
5) La posta elettronica non deve essere utilizzata per la creazione, distribuzione o rilancio di messaggi di disturbo o offensivi, commenti sull'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, lo stato di salute o la disabilità, il genere, il colore dei capelli, l'età, la vita o l'orientamento sessuale della persona. I dipendenti che dovessero ricevere messaggi con queste tipologie di contenuto da qualsiasi dipendente devono segnalare immediatamente la questione al diretto superiore.
6) La posta elettronica non deve essere utilizzata per inviare messaggi massivi ad una moltitudine di utenti, in particolare per diffondere locandine, inviti o pubblicizzare eventi, prediligendo la pubblicazione sul sito intranet dell'organizzazione nella sezione *news* o eventi, a meno di informazioni particolarmente importanti o urgenti, e comunque su specifica autorizzazione della Direzione.
7) L'utilizzatore non può utilizzare la posta elettronica dell'organizzazione per inviare documenti contenenti dati personali, specie se di natura particolare, che lo riguardano o che riguardino soggetti terzi.
8) La posta elettronica ordinaria o e-mail secondo la recente giurisprudenza[3], rispetto a quanto previsto dal Regolamento (UE) 2014/910 eIDAS (*electronic IDentification Authentication and Signature*) e

[3] Sentenze n. 14716/2011 e n. 11402/2016 Tribunale di Milano

dalle conseguenti modifiche al D.lgs. n. 82/2005 CAD (Codice dell'Amministrazione Digitale) ha validità giuridica e rilevanza probatoria[4], è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

9) Un messaggio di posta elettronica convenzionale inviato allo stesso dominio (@<ORGANIZZAZIONE>.it) ha un livello di sicurezza mediamente elevato; nel caso di invio ad altri domini anche se istituzionali (ministeri, regioni, comuni, ecc.) il livello di sicurezza potrebbe essere equiparabile alla semplice cartolina postale. Per questo motivo è necessario verificare il destinatario, soprattutto se multiplo, e in particolare il contenuto della comunicazione (testo e allegati).
10) Alla fine della sessione di lavoro è necessario effettuare sempre la disconnessione (log-out) dal sistema di posta.
11) L'indirizzo di posta elettronica non deve essere utilizzato per la registrazione a siti web che non siano in qualche modo legati alle attività svolte dagli utilizzatori intestatari nell'organizzazione, anche al fine di limitare lo spam.
12) Non lanciare mai i link di annullamento alle sottoscrizioni delle e-mail considerate indesiderate (il cd. "*unsubscribe*"), al fine di ridurre il rischio di conferma dell'esistenza e utilizzo della e-mail.
13) Al fine di garantire la corretta coerenza comunicativa dell'organizzazione, è vietato modificare il *footer* (parte finale del messaggio di default) rispetto allo standard dell'organizzazione.
14) Tutti i messaggi di posta elettronica devono riportare in calce la firma del mittente secondo lo standard dell'organizzazione, con font e dimensioni come di seguito riportato:

Rossi Mario	[font Calibri 11 punti in **grassetto**]
Ruolo e Area di appartenenza	[font Calibri 10 punti normale]
Denominazione Organizzazione	[font Calibri 10 punti normale]
Indirizzo	[font Calibri 10 punti normale]
Telefoni (fisso e mobile organizzazione)	[font Calibri 10 punti normale]

Non sono ammesse personalizzazioni differenti.

15) I sistemi di sicurezza come firewall e antispam garantiscono con discreta probabilità che le e-mail consegnate siano esenti da pericoli. È sempre a carico dell'utilizzatore la verifica ultima di:
    a. **Mittente**: deve essere conosciuto (da verificare l'indirizzo effettivo e non la semplice denominazione); esempio da evitare e marcare come spam è il mittente service145@mail.145.com;
    b. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo *phishing*; la verifica può essere fatta posizionando il cursore del mouse sul link per visualizzare la reale destinazione (ad esempio evitare di fare click su link del tipo http://amazon.net.ru);
    c. **Allegati**: diffidate dei file con estensione multipla o senza estensione o con denominazione estranea alle attività o mansioni svolte abitualmente (es. 'Si allega fattura');
    d. **Contenuti**: scrittura con errori grossolani (traduzione da sistemi automatici), riferimenti alla chiusura di un conto o di un servizio, parole come URGENTE, richieste di dati personali o di password, file che non sono mai stati richiesti o con estensioni sospette.
16) Nei casi dubbi non aprire le e-mail o i contenuti e contattare il supporto tecnico che provvederà alla verifica secondo le procedure di sicurezza.

[4] Dalla definizione CAD di "firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica", l'utilizzo delle credenziali di accesso alla casella di posta elettronica vale a qualificare l'utente e costituisce pertanto una firma elettronica semplice, non avanzata né qualificata, ma comunque non giuridicamente irrilevante e sotto il profilo probatorio liberamente valutabile in giudizio

17) È vietato il *forward* o rilancio della posta sui dispositivi mobili (es. smartphone e tablet) personali. Il *forward* dei messaggi è permesso solamente sui dispositivi mobili di proprietà dell'organizzazione, agli utilizzatori specificatamente autorizzati.
18) L'utilizzo di *forward* di posta automatico dell'organizzazione su altri sistemi (es. Gmail) è vietato; questo al fine di garantire un adeguato livello di sicurezza dei contenuti dei messaggi come, ad esempio, gli allegati contenenti dati personali o riservati inviati dal mittente che, non essendo a conoscenza del rilancio, non adotta le misure necessarie alla protezione dei contenuti prevista per trasferimenti al di fuori dell'Unione Europea.
19) La posta elettronica fornita dall'organizzazione non può essere utilizzata per scopi personali estranei all'attività lavorativa. Viceversa, è vietato utilizzare o fornire e-mail personali per scambiare informazioni, contenuti o allegati legate all'attività lavorativa.
20) L'invio di file tramite link ai sistemi di hosting è permesso solo se i file sono criptati e le chiavi di criptazione sono condivise su altro media. Le procedure di criptazione sono disponibili nella intranet dell'organizzazione.
21) Non consultare la posta elettronica dell'organizzazione presso Internet point, Wi-Fi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar).
22) Le raccomandazioni o indicazioni inviate via e-mail non devono essere seguite poiché nella maggior parte dei casi si tratta di virus HOAX (cd. bufale). In caso di dubbi contattare il supporto tecnico SIA.
23) Marcare come spam le e-mail che appaiono come *scam* ovvero tentativi di truffa pianificata con metodi di ingegneria sociale (in genere nella e-mail si promettono enormi guadagni in cambio di somme di denaro da anticipare).
24) Le e-mail che richiedono l'attivazione delle macro di MS-Word o MS-Excel prima del download degli allegati devono essere immediatamente marcate come spam.
25) Non attivare mai i link presenti nelle cosiddette e-mail di reset della password, né fornire mai le credenziali di autenticazione per nessun motivo.
26) Non rispondere e inoltrare e-mail delle cosiddette catene di Sant'Antonio o rispondere alle e-mail di spam.
27) La policy della posta elettronica prevedono le seguenti limitazioni:
    a. Dimensione massima della casella di posta elettronica è paria 2.5 GB (evitare di trasformare il sistema di posta elettronica in sistema di archiviazione), mentre è pari a 1 GB per gli utenti base;
    b. Dimensione massima degli allegati inviati o ricevuti pari a 25 MB;
    c. Limite massimo di destinatari contemporanei pari a 50 a meno delle liste di distribuzione;
    d. Limite delle *Address list* creabili pari a 1000;
    e. Limite del *forwarding* pari a 10 recipienti;
28) Gli allegati inviati via e-mail contenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste in questi casi. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (es. via telefono).
29) Le e-mail contenenti evidenze di reati penali devono essere prima visionate dal personale tecnico dei Sistemi Informativi e poi, se del caso, informate le autorità per la presentazione della denuncia; questo al fine di evitare falsi allarmi.
30) In casi particolari, di emergenza o semplicemente nel caso non si ricevano le risposte nei tempi attesi, è possibile effettuare la cosiddetta *escalation* ovvero scrivere direttamente al diretto superiore del primo destinatario. Le comunicazioni in modalità *escalation*, se considerate inutili, espongono il mittente alle sanzioni disciplinari previste.
31) L'invio a più soggetti di un messaggio di posta elettronica può essere effettuato in "CC" (Carta Carbone) soltanto nel caso di destinatari appartenenti allo stesso dominio di (@<ORGANIZZAZIONE>.it); nel caso di invio a più destinatari è FONDAMENTALE utilizzare il "CCN"

(Carta Carbone Nascosta) in modo che i singoli non possano in nessun modo venire a conoscenza degli indirizzi degli altri destinatari.

32) L'invio di messaggi di posta elettronica a sottogruppi numerosi oppure a tutti i destinatari del dominio di posta è riservato alla Direzione e ai soggetti specificamente autorizzati. Eventuali forzature del sistema potranno essere sanzionate ai sensi del presente Regolamento.
33) Dopo la cessazione del rapporto di lavoro dell'utilizzatore, i contenuti della casella di posta elettronica sono conservati per ulteriori 180 giorni (senza considerare le tempistiche di *Retention* del sistema di backup) ai soli fini di tutela dei diritti in sede giudiziaria, senza possibilità di accesso se non da parte degli Amministratori del sistema di posta.
34) In nessun caso è possibile richiedere copia delle e-mail inviate o ricevute poiché relative al patrimonio informativo dell'organizzazione e contenenti comunicazioni esclusivamente legate al rapporto di lavoro.
35) L'utilizzatore del sistema di posta, in caso di sospensione del servizio per ferie o malattia, è tenuto autonomamente all'impostazione del messaggio di risposta automatica delle e-mail e alla richiesta di inoltro ai colleghi oppure al diretto superiore.
36) In caso di assenza dell'utilizzatore intestatario dell'account e-mail e in presenza di specifiche necessità istituzionali di accesso ai messaggi di posta, il diretto superiore può richiedere ai Sistemi Informativi l'accesso al singolo messaggio o all'intera cartella, il *forward* momentaneo o definitivo dell'account di posta su altro indirizzo. Di tale attività deve essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.
37) Nel caso si riceva una e-mail visibilmente contraffatta da un collega, è necessario informare immediatamente il supporto tecnico.
38) Nel caso la marcatura come messaggio indesiderato di un insieme ricorrente di messaggi di spam non riduca il problema, sono attivabili i cosiddetti filtri personalizzati, in grado di marcare automaticamente tipologie di e-mail indesiderate; nella Intranet sono disponibili le istruzioni per l'attivazione della funzionalità.
39) Al fine di contenere lo spazio di memoria del server di posta è necessario conservare solo e-mail rilevanti per la propria attività. Le e-mail non più utili devono essere eliminate (soprattutto se con allegati di dimensioni elevate).
40) L'utente deve organizzare la propria casella di posta in modo tale che ci sia una separazione tra l'archivio corrente e quello storico secondo la regola:

    Archivio on line
    Posta in Arrivo – 2019
    2020
    2021

    I dati meno recenti potranno così essere memorizzati in modo automatico in contenitori a prestazioni meno elevate.
41) Nel caso di comportamenti anomali del personal computer, evidenziati a seguito dell'apertura di una e-mail, di un click su un link o di un download di un file, è necessario:
    a. staccare immediatamente il cavo di rete;
    b. lasciare il computer acceso;
    c. segnalare immediatamente l'accaduto ai Sistemi Informativi e al proprio Dirigente.
42) I documenti che generano, o fanno parte di, processi che hanno valenza amministrativa nonché quelli aventi efficacia esterna rispetto all'organizzazione (come determine, delibere, decreti, verbali, circolari e contratti), in quanto documenti di preminente carattere giuridico-probatorio e fondamentali per la gestione dei procedimenti amministrativi, possono essere inviati via posta elettronica soltanto dopo essere stati oggetto di registrazione di protocollo.

43) La ricezione di eventuali messaggi che rappresentano istanze o dichiarazioni da parte di terzi, presentate nelle modalità, così come previste all'art. 65 del CAD (es. richiesta con allegata copia di un documento di identità), devono essere girate al sistema di protocollo per la dovuta procedura di registrazione e assegnazione.

Art. 10. - BYOD (*bring-your-own-device*) - Dispositivi di proprietà personale

1) I cosiddetti BYOD (*Bring Your Own Device*, letteralmente "porta il tuo dispositivo") possono essere utilizzati soltanto come sistemi isolati non collegati alla rete dell'organizzazione, a meno del Wi-Fi con accesso di tipo *guest* (se presente). I sistemi di monitoraggio effettuano controlli automatici continui e segnalano al personale tecnico i sistemi e i dispositivi non catalogati e non autorizzati che abbiano effettuato un collegamento diretto alla rete locale dell'organizzazione (LAN). Eventuali sistemi o dispositivi non autorizzati collegati alla rete dell'organizzazione saranno bloccati e considerati come attacco al sistema informatico, segnalati alla Polizia Postale e delle Comunicazioni per la denuncia di reato di accesso abusivo a sistema informatico ai sensi dell'Art. 615/ter del Codice penale.
2) È severamente vietato il collegamento alla rete dell'organizzazione di sistemi o dispositivi non distribuiti ufficialmente dai Sistemi Informativi. Il personale che effettuerà il collegamento diretto alla rete dell'organizzazione (sono escluse i Wi-Fi pubblici) sarà soggetto a sanzioni disciplinari. Saranno inoltre addebitati all'utilizzatore eventuali costi di ripristino o ulteriori danni che dovessero originarsi da un collegamento non autorizzato. Rientrano nei dispositivi del presente comma modem, router, switch, dispositivi wireless, Bluetooth o qualsiasi altro dispositivo che possa in qualche modo ampliare la superficie di esposizione e quindi i rischi connessi.
3) Il collegamento alla rete Wi-Fi pubblica dell'organizzazione (ove disponibile) dei dispositivi di proprietà personale come laptop, tablet o smartphone è possibile seguendo la specifica procedura di autorizzazione, registrazione e autenticazione.
4) In conformità alla normativa vigente in tema di protezione dei dati personali è vietato salvare sui BYOD i dati personali, specialmente se di natura particolare, raccolti durante le attività lavorative se non sono attivi livelli di sicurezza equiparabili a quelli dell'organizzazione (antivirus con basi aggiornate, firewall locale attivo, aggiornamento del sistema operativo e dei componenti, assenza di software copiato o "*crackato*").
5) È vietato l'utilizzo di dispositivi personali per scattare foto durante le attività lavorative; è altresì severamente vietata la loro diffusione sui canali social.
6) In nessun caso è possibile installare software con licenza di proprietà dell'organizzazione sui dispositivi BYOD.
7) Il trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione personali contenenti dati sensibili è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
8) Nell'ipotesi di smarrimento o furto di un dispositivo BYOD contenente dati personali riconducibili all'organizzazione titolare del trattamento dei dati, è obbligatorio comunicare l'accaduto al DPO/RPD per l'attivazione della procedura di *Data Breach.*

Art. 11. - Navigazione Internet

1) Internet è la fonte di informazioni e documentazione più vasta esistente, quindi irrinunciabile tanto per il personale operativo quanto per il personale amministrativo. L'interoperabilità tra enti pubblici passa sia attraverso il Sistema Pubblico di Connettività sia attraverso la rete Internet, con una serie di servizi indispensabili al funzionamento della macchina amministrativa. L'ente mette a disposizione

questo servizio a patto che se ne faccia buon uso ovvero che le finalità di navigazione siano connesse esclusivamente all'attività lavorativa.

2) A meno di specifica autorizzazione, è vietato navigare in tutti i siti web appartenenti alle categorie previste nell'Appendice *Content Filtering Rating Categories,* sia dalla rete locale che WiFi, navigare per fini ludici o personali, effettuare upload o download di file e documenti non connessi all'attività lavorativa, effettuare streaming audio o video (es. radio o tv via Internet), telefonare (es. Skype), effettuare chat on-line se non specificatamente autorizzati.
3) È tassativamente vietata la navigazione in siti Internet palesemente incompatibili con le finalità dell'organizzazione, che istighino a comportamenti illegali, che consentano o siano a rischio di diffusione di virus, cavalli di Troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, *hacking* o pirateria informatica a danno dei computer di altri utenti interni o esterni al perimetro dell'organizzazione.
4) È inoltre vietato navigare in siti web che possano comportare nei sistemi deputati al monitoraggio e alla protezione della connessione Internet, trattamenti involontari di dati personali di tipo sensibile riconducibili agli utilizzatori del servizio (esempio convinzioni religiose, politiche, stato di salute, vita sessuale).
5) La navigazione web non è esente da rischi, nonostante siano già attivi diversi strumenti di protezione; gli impatti potrebbero non essere legati al singolo computer ma interessare parte o addirittura l'intero patrimonio informativo dell'organizzazione, con risvolti imprevedibili sulla continuità stessa dei servizi e danni reputazionali e di immagine. Per queste motivazioni è sempre in capo al singolo utilizzatore la verifica di:
    a. **Indirizzo del sito web**: è necessario verificare più di una volta l'indirizzo completo (attenzione ai siti web che appaiono simili ma non lo sono: www.<organizzazione><città>.it o www. <organizzazione.<*sitowebstrano*>.it; la dimensione del font della barra dell'indirizzo non aiuta);
    b. **Certificato**: evitare i siti non sicuri (con protocollo http) e nel caso di siti in https fare attenzione alla perfetta corrispondenza del certificato con intestazione e indirizzo del sito web in questione;
    c. **Riferimenti**: i siti dei cosiddetti *scammer* o truffaldini non riportano né l'indirizzo della sede né tantomeno numeri telefonici o altri riferimenti;
    d. **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto nell'aspetto grafico); questo al fine di evitare attacchi di tipo *phishing*; la verifica può essere effettuata posizionando il cursore del mouse sul link in modo da visualizzare la destinazione reale (ad esempio evitare di fare click su link del tipo www.organizzazzione.it nel caso vi sia un rimando ad altro sito, ad esempio: www.<altrositostrano>.it);
    e. **Download**: evitare di scaricare da siti non ufficiali qualsiasi documento, software applicativo, driver o componente aggiuntivo (*plug-in* del browser o componenti "dinamici" come ActiveX o funzioni JavaScript), includendo anche le app per dispositivi *mobile*;
    f. **Contenuti**: verificare la presenza di errori sintattici grossolani (dovuti a traduzione automatiche) al fine di riconoscere siti non ufficiali (tecnicamente denominati *fake*);
    g. **Verifiche web**: attraverso i motori di ricerca è possibile trovare altre informazioni sul sito che possono aiutare nell'identificazione; provare ad effettuare una ricerca web con la denominazione del sito seguita dalle parole "opinioni" o "recensioni" (su un motore <altrositostrano>.it opinioni).

    Nei casi dubbi non aprire il sito web o interrompere la navigazione, chiudere il browser e, nel caso il sistema inizi ad avere comportamenti singolari, disconnettere il sistema dalla rete locale e contattare immediatamente il supporto tecnico che provvederà ad effettuare le verifiche secondo le procedure di sicurezza.

6) L'utilizzo moderato e sporadico degli strumenti informatici dell'organizzazione per finalità private è tollerato, solo nel caso che questo non comporti nocumento all'attività lavorativa.
7) I rischi derivanti dall'utilizzo delle informazioni personali (ad es. numeri di carte di credito) durante la navigazione web estranea alle attività lavorative, sono sempre in capo all'utilizzatore. Il Titolare non potrà essere ritenuto responsabile di eventuali danni dovuti a perdite di riservatezza, integrità o disponibilità di dati personali inviati in sessioni effettuate con strumenti dell'organizzazione e in orario di lavoro.
8) L'acquisizione, conservazione, trasmissione o diffusione di file dal contenuto illegale, discriminatorio per origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, o appartenenza sindacale, stato di salute o disabilità, genere, colore dei capelli, età, vita sessuale o orientamento sessuale della persona è vietato. Eventuali abusi o contenuti illegali che si dovessero evidenziare durante la navigazione devono essere comunicati al supporto tecnico per le valutazioni del caso.
9) L'acquisizione, conservazione, trasmissione o diffusione di materiale che violi il diritto d'autore, i marchi, i segreti commerciali o i diritti di brevetto di qualsiasi persona o organizzazione è vietato. Tutti i materiali pubblicati su Internet sono protetti da copyright e/o brevettati, salvo diversa indicazione[5] (Legge 633/1941 – "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).
10) La trasmissione di informazioni proprietarie, riservate o altrimenti sensibili, contenenti dati personali di tipo particolare è vietata. Solo se specificatamente autorizzato, l'utente può effettuare l'invio/upload a condizioni di adottare controlli specifici e livelli di protezione elevati forniti dalla criptazione.
11) La larghezza di banda della rete locale (interna) dell'organizzazione come anche la connettività Internet è una risorsa condivisa e limitata. Considerato che gli utilizzi indebiti di un singolo utilizzatore potrebbero impattare sulle attività degli altri, sono adottate delle politiche di gestione della banda in funzione delle tipologie di attività svolte che garantiscono il massimo delle prestazioni possibili in funzione delle priorità (*packet shaping*).
12) Le attività di navigazione internet degli utilizzatori sono monitorate da un sistema automatico che verifica i seguenti parametri:
    a. Quantità di dati scaricati giornalmente e mensilmente (inferiore ai 500 Mbyte/giorno);
    b. Tipologie di siti visitati (in vista aggregata e conformi alle politiche di *content filtering*);
    c. Tempistiche totali di navigazione Internet.

    Eventuali comportamenti degli utilizzatori anomali, non conformi o superiori ai parametri generali sopra riportati, quindi non funzionali al corretto funzionamento del servizio, potranno comportare la disattivazione automatica dell'account di accesso per motivi di sicurezza o al fine di garantire la necessaria continuità operativa.
13) In conformità alla normativa sulla protezione dei dati personali e perseguendo i principi generali ovvero necessità, correttezza, pertinenza e non eccedenza, è garantita la sovra-registrazione dei dati del traffico Internet dell'utilizzatore, la cui conservazione non sia necessaria (è attivata la cd. rotazione dei log file).
14) La conservazione dei file di registrazione della navigazione degli utilizzatori è limitata a 10 giorni, che è considerato il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, fatti salvi in ogni caso specifici obblighi di legge. Sono esclusi dalle regole di conservazione i dati aggregati di navigazione.

[5] Ad esempio, le 6 licenze di tipo Creative Commons, definite dalla combinazione di quattro attributi che permettono di stabilire esplicitamente quali siano i diritti riservati, modificando la regola di default in cui tutti i diritti sono riservati.

Art. 12. - Utilizzo del personal computer (desktop) o del portatile (laptop)

1) La continuità dei servizi è strettamente legata alla normale operatività di tutti i dispositivi della catena tecnologica, a partire dalla postazione di lavoro. Utilizzi impropri dei dispositivi e delle apparecchiature possono produrre effetti indesiderati e compromettere il funzionamento che, in casi particolari, potrebbe causare danni alle persone. L'utilizzatore di sistemi e servizi IT sarà ritenuto responsabile per i costi di riparazione nel caso che il danno sia causato da uso improprio o da negligenza.
2) È vietato modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete dell'organizzazione e all'alimentazione elettrica, da parte dell'utilizzatore o di personale esterno, senza specifica autorizzazione del personale del servizio di supporto tecnico SIC. [Necessario seguire specifica procedura]
3) Non è consentito l'uso o l'installazione di software applicativi diversi da quelli distribuiti ufficialmente dai Sistemi Informativi (ai sensi del D.lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore), inclusi nel catalogo dei servizi e nella *white list.* Sono periodicamente effettuati controlli e, in caso di presenza di compenti o applicazioni non autorizzate, il personale dei Sistemi Informativi procede con la disinstallazione, anche in modalità da remoto.
4) È vietato conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, e-mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo se di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.
5) Il trasporto al di fuori del perimetro dell'organizzazione di dispositivi di memorizzazione contenenti dati personali e sensibili è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.
6) L'utilizzatore di sistemi e servizi IT è invitato alla immediata segnalazione al servizio di supporto tecnico di eventuali danni, perdita di funzionalità parziale o totale dei dispositivi o delle apparecchiature.
7) Nel caso di malfunzionamenti o comportamenti inusuali dei sistemi, configurabili come compromissioni, l'utilizzatore è tenuto a:
    a. scollegare immediatamente il sistema dalla rete locale;
    b. segnalare l'accaduto al proprio superiore;
    c. aprire una richiesta di intervento (ticket) ai Sistemi Informativi.
8) Eventuali specifiche indicazioni o istruzioni fornite dal personale di supporto tecnico devono essere rispettate al fine di garantire il miglior funzionamento possibile dei sistemi, dei dispositivi e delle risorse condivise.
9) Concluse le attività lavorative o nel caso di momentanea assenza o allontanamento dalla postazione di lavoro, l'utilizzatore di sistemi e servizi IT è tenuto alla disconnessione dei servizi e degli applicativi attivi o alla completa disconnessione/arresto del sistema (Windows-l (elle), blocco dell'utilizzatore connesso oppure Start – Arresta / Disconnetti).

Art. 13. - Sistemi e dispositivi di acquisizione e stampa

1) L'organizzazione prevede l'utilizzo di sistemi e dispositivi di acquisizione e stampa dei documenti. La vigente normativa in tema di digitalizzazione prevede però l'acquisizione nativa dei documenti digitali, la loro comunicazione, elaborazione sempre in formato digitale e, infine, la conservazione sostitutiva, sempre digitale[6]. In attesa di completare il processo di digitalizzazione dei documenti e, parallelamente, la revisione dei processi amministrativi, è possibile stampare esclusivamente la

[6] Decreto della Presidenza del Consiglio del 13 novembre 2014, che all'articolo 17 comma 2

documentazione strettamente necessaria, avendo cura di ritirarla immediatamente, in modo da evitare diffusione di informazioni, anche di tipo riservato.

2) In ogni caso è vietata la stampa o acquisizione di documenti personali dell'utilizzatore, estranei all'attività lavorativa svolta.
3) A meno di impossibilità tecnica o amministrativa, i documenti dovrebbero essere sempre stampati in modalità fronte-retro.
4) La carta deve essere caricata negli appositi alloggiamenti evitando piegature o caricamenti parziali, avendo cura di sfogliare leggermente senza disallineamenti dei bordi al fine di evitare inceppamenti.
5) In ogni caso l'utilizzatore non è autorizzato a smontare il dispositivo anche nel caso di inceppamenti della carta lungo il percorso di stampa che dovranno essere gestiti tramite segnalazione ai sistemi informativi o al riferimento tecnico del dispositivo.

Art. 14. - Utilizzo delle cartelle di rete, collegate e condivise

1) Le cartelle di rete, collegate e condivise, sono di 3 tipi:
    a. Cartella ad accesso personale (Disco X:) dove salvare i documenti ancora in lavorazione o non ancora da condividere;
    b. Cartella ad uso delle Aree (Disco Y:) per la condivisione tra gli utilizzatori appartenenti allo stesso gruppo/ufficio;
    c. Cartella progetto (Disco Z:) ad uso combinato tra più Aree per la condivisione interdipartimentale;
    d. Cartella scansioni (Disco S:) per la memorizzazione temporanea dei files scansionati dai dispositivi multifunzione;
    e. File hosting dell'organizzazione per la condivisione via web.
2) L'utilizzatore dovrebbe utilizzare la Cartella ad accesso personale per la memorizzazione dei documenti e di tutte le informazioni riguardanti il cosiddetto *Roaming Profile* e *Folder redirection*.
3) La politica di sicurezza dell'organizzazione non prevede la possibilità per gli utenti di salvare informazioni di alcun tipo sui dischi locali; da ricordare come i file salvati in locale sui personal computer non sono replicati (non è previsto un backup dei dati contenuti sui singoli PC) e in caso di problemi ai dispositivi di memorizzazione potrebbero andare irrimediabilmente persi.
4) Nelle cartelle condivise (es. ad uso delle Aree) è possibile impostare stratificazioni dei permessi (es. un gruppo di utenti legge e un altro scrive su una cartella, mentre il resto è ad accesso libero).
5) Le cartelle collegate e condivise sono replicate in sicurezza (backup) tutti i giorni; è garantita una *retention* (tempo di conservazione delle copie) generalmente di 2 settimane (verificare con i Sistemi informativi le singole garanzie di conservazione rispetto ai servizi erogati);
6) È vietato conservare file protetti dal diritto d'autore nelle cartelle condivise, come anche in tutti gli altri dispositivi di memorizzazione dell'organizzazione.
7) I marchi, i segreti commerciali o i diritti di brevetto devono essere conservati con particolari accortezze e ad accesso ristretto. Contattare il supporto tecnico per delucidazioni a riguardo.
8) Gli utilizzatori hanno invece il compito di:
    a. Contenere lo spazio disco occupato entro le quote assegnate (quota utente X: base pari a 20 Gbyte eventualmente estendibile per casi particolari);
    b. Eliminare i file non più utilizzati o duplicati (es. file1.vers1, file1.vers2);
    c. Evitare la duplicazione delle informazioni già contenute in applicativi specifici dell'organizzazione (export dei dati per successiva elaborazione su Excel, import dei dati in database Access).
9) In caso di assenza dell'utilizzatore intestatario della Cartella ad accesso personale (Disco X:) e in presenza di specifiche necessità istituzionali di accesso, il diretto superiore può richiedere ai Sistemi

Informativi l'accesso al singolo file o all'intera cartella. Di tale attività deve essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

Art. 15. - *Cloud computing* e servizi IT esterni

1) L'acquisizione di servizi basati su tecnologia cloud come IaaS, PaaS e SaaS devono essere conformi alla normativa nazionale e alle Politiche di approvvigionamento che prevedono per servizi tecnologici l'autorizzazione da parte dei Sistemi Informativi dell'organizzazione. Considerati i possibili impatti sulla protezione dei dati è necessario informare preventivamente anche il DPO/RPD.
2) L'utilizzo di sistemi basati su tecnologia cloud o web non autorizzati e tracciati è considerato un data breach con tutti i risvolti sanzionatori ed eventualmente risarcitori a carico dell'utilizzatore.
3) Ai sensi di quanto previsto dalle Circolari 2 e 3 2018 di AgID non è possibile acquisire servizi in modalità SaaS se non qualificati dalla stessa AgID e pubblicati nel rispettivo Marketplace.

Art. 16. - Utilizzo Reti Wi-Fi pubbliche

1) Per ragioni di sicurezza, non devono essere utilizzate reti Wi-Fi pubbliche con l'opzione di protezione WEP ma soltanto WPA o WPA2.
2) Utilizzare la connessione Wi-Fi pubblica solo per effettuare navigazione informativa; non accedere mai alle piattaforme dell'organizzazione. Sono inoltre sconsigliati l'effettuazione di transazioni di tipo sensibile (ad es. acquisti o transazioni bancarie).

Art. 17. - Sistemi di Sicurezza

1) L'organizzazione al fine di tutelare il patrimonio informativo e la continuità dei servizi, utilizza dei dispositivi di sicurezza con i quali controlla e monitora in modalità aggregata l'attività dei sistemi e indirettamente anche quella degli utilizzatori. Al fine di poter valutare i livelli di servizio erogati ed effettuare attività di ricerca forense a seguito di eventuali attacchi, tutte le attività dei sistemi e degli utilizzatori sono salvate in appositi registri o file di log, ai quali può accedere solamente il personale autorizzato e specificatamente nominato Amministratore di Sistema.
2) L'accesso ai file di log da parte del personale nominato Amministratore di Sistema può avvenire per attività di normale manutenzione, a seguito di malfunzionamenti o di degradamento dei livelli di servizio, in funzione di specifiche segnalazioni oppure nel caso di richiesta da parte dell'Autorità Giudiziaria.
3) La scelta dei criteri di protezione nei sistemi di sicurezza è tesa al giusto equilibrio tra performance e livello di salvaguardia, proporzionale ai rischi connessi con la tipologia di informazioni trattate. In alcuni casi, i controlli possono interferire con l'esperienza dell'utilizzatore di sistemi e servizi IT, ad esempio con blocchi nella navigazione, accessi non concessi, segnalazione di attività non permesse. L'utilizzatore di sistemi e servizi IT è invitato a segnalare gli elementi che ritiene possano essere migliorati (ad es. falsi positivi).
4) L'utilizzatore di sistemi e servizi IT non deve modificare, aggirare, disabilitare i controlli di sicurezza. Eventuali attività ritenute sospette comporteranno l'immediata disattivazione dell'account di accesso ai sistemi e servizi (questo poiché è impossibile per un sistema automatico stabilire con certezza se il problema è, o meno, riconducibile ad una compromissione, presentandosi come rischio inaccettabile e non risolvibile con altri mezzi).
5) L'accesso alle infrastrutture di rete, alle attrezzature e strumenti informatici è permesso al solo personale autorizzato; il personale privo di autorizzazione non può effettuare l'accesso, anche se accompagnato, senza preliminare autorizzazione e registrazione.
6) I sistemi o i dispositivi compromessi a seguito di attacco devono essere ripristinati dal personale dei Sistemi Informativi seguendo le procedure previste; la delega a terza parte necessita di specifica approvazione da parte di un soggetto Designato.

7) I sistemi e gli applicativi necessitano di continui aggiornamenti che permettono di mantenere l'intera infrastruttura ad un adeguato livello di protezione e sicurezza, eliminando i difetti o le vulnerabilità note. Nonostante tutte le accortezze, alcuni aggiornamenti richiedono molto tempo, rallentano il sistema o possono esigere un riavvio. L'utilizzatore di sistemi e servizi IT deve seguire quanto richiesto dal sistema o dall'applicazione nel più breve tempo possibile al fine di ridurre i rischi legati allo specifico aggiornamento.

Art. 18. - Pubblicazione di informazioni sui siti web istituzionali e Social media

1) L' Istituto Scolastico Comprensivo Castel di Lama 1 utilizza i propri siti web e i social media con finalità istituzionali e di interesse generale per informare, comunicare, ascoltare e per consentire una relazione più diretta e una maggiore partecipazione dell'utenza alle attività svolte.
2) Attualmente la comunicazione del Istituto Scolastico Comprensivo Castel di Lama 1 avviene attraverso le pagine tematiche presenti su:
    - Portale Nuvola
    - Sito istituzionale medialama.edu.it

    In futuro non sono escluse ulteriori affiliazione ai social media (la lista delle piattaforme attive è pubblicata nell'header e/o nel footer del sito web dell'organizzazione) o la registrazione di specifici domini web.
3) I contenuti che sono pubblicati sui siti web istituzionali e sui social possono comprendere comunicazioni sulle attività e i servizi erogati, comunicati stampa, pubblicazioni e documenti ufficiali, novità normative, informazioni su iniziative ed eventi di settore, immagini e video istituzionali e relativi a eventi a cui l'organizzazione partecipa.
4) I canali producono propri contenuti testuali, fotografie, informazioni grafiche, video e altri materiali multimediali che sono da considerarsi in licenza *Creative Commons* CC BY-ND 3.0 [Attribuzione – Non opere derivate http://creativecommons.org/licenses/by-nd/3.0/it/deed.it]: possono essere riprodotti liberamente, ma devono sempre essere accreditati al canale originale di riferimento.
5) I commenti e i post degli utenti, presentati preferibilmente con nome e cognome non fittizi, rappresentano l'opinione dei singoli e non quella dell'organizzazione, che non può essere ritenuta responsabile della veridicità o meno di ciò che viene postato sui canali da terzi, entità giuridiche o naturali.
6) I partecipanti alle discussioni sui social network sono responsabili dei contenuti pubblicati e delle opinioni espresse. Non sono comunque tollerati insulti, volgarità, offese, minacce. Devono essere evitati riferimenti a fatti o a dettagli privi di rilevanza pubblica, atteggiamenti violenti, offensivi o discriminatori rispetto al genere, orientamento sessuale, età, religione, convinzioni personali, origini etniche, disabilità. Messaggi contenenti dati personali (indirizzi e-mail, numeri di telefono, numeri di conto corrente, indirizzi, etc.), o dati di tipo particolare, come anche informazioni riservate o confidenziali relative all'organizzazione, saranno rimossi a tutela delle persone interessate.
7) L'attività di moderazione da parte dell'amministratore della piattaforma o del social può avvenire solo a posteriori in un momento successivo alla pubblicazione; l'attività è finalizzata, unicamente, al contenimento di eventuali comportamenti contrari alle norme d'uso, garantendo a tutti il diritto di intervenire ed esprimere la propria libera opinione. L'operatore può utilizzare il *nickname* previsto oppure utilizzare il proprio nominativo e, in tal caso, è tenuto a rivelare anche la sede di lavoro e la mansione ricoperta.
8) Non sono tollerati comportamenti da cosiddetti *hater*, con insulti, turpiloquio, minacce o atteggiamenti che ledano la dignità personale, i diritti delle minoranze e dei minori, i principi di libertà e uguaglianza o altri principi costituzionalmente riconosciuti ed in particolare:

a. Contenuti che promuovono, favoriscono, o perpetuano la discriminazione sulla base del sesso, della razza, della lingua, delle opinioni politiche, credo religioso, età, stato civile, nazionalità, disabilità fisica o mentale, orientamento sessuale;
b. Contenuti sessuali o link (collegamenti) a contenuti sessuali;
c. Pubblicità evidente o sollecitazioni commerciali;
d. Incoraggiamento ad attività illecite;
e. Informazioni che possono tendere a compromettere la sicurezza o la sicurezza dei sistemi pubblici;
f. Contenuti che violino l'interesse di una proprietà legale o di terzi;
g. Commenti o post che presentino dati sensibili in violazione della normativa sulla protezione dei dati personali;
h. Sono inoltre scoraggiati e comunque soggetti a moderazione commenti e contenuti dei seguenti generi:
    i. Spam, commenti non pertinenti agli argomenti trattati (*off topic*);
    ii. Osservazioni pro o contro campagne politiche o indicazioni di voto;
    iii. Linguaggio o contenuti offensivi;
    iv. Commenti e i post scritti per disturbare la discussione, offendere chi gestisce e modera i canali social;
    v. Interventi inutili o inseriti ripetutamente.

9) Gli utilizzatori che dovessero violare ripetutamente le condizioni sopra riportate o quelle contenute nelle specifiche policy degli strumenti adottati, potranno essere "bannati" o bloccati al fine di impedirne ulteriori interventi.
10) Le attività ritenute illegali saranno immediatamente comunicate alle autorità competenti.
11) **Prescrizioni per il personale**. Il personale che accede in generale ai Social Network con propri account personali, considerato che lo stesso può essere facilmente identificato dagli altri utenti come un dipendente dell'organizzazione, deve impegnarsi a mantenere un comportamento eticamente corretto e allineato alla presente politica generale.
    Pertanto, il personale è tenuto ad osservare le seguenti prescrizioni:
    a. in caso di intervento in argomenti riguardanti anche marginalmente l'Organizzazione o il suo operato, deve specificare che trattasi di PROPRIA opinione, non effettuando tale azione nelle veci dell'Organizzazione;
    b. deve evitare di rilevare informazioni e problematiche riguardanti l'ambito lavorativo e, qualora si trovi coinvolto in discussioni critiche o dannose per l'Organizzazione è invitato a informare il responsabile della comunicazione e dei Social Media;
    c. ogniqualvolta noti degli errori o delle presunte non conformità rispetto alla presente Politica deve effettuare specifica segnalazione al responsabile della comunicazione e dei Social Media;
    d. prima di procedere con la condivisione di notizie, fatti, eventi, punti di vista, deve necessariamente verificare la veridicità della fonte;
    e. se previsto nella gestione dei profili della piattaforma o durante le conversazioni, è necessario riportare ruolo e mansione svolta nell'Organizzazione;
    f. richiedere supporto ai Sistemi Informativi al fine di poter impostare un preciso livello di privacy e sicurezza in merito ai contenuti;
    g. al fine della massima diffusione è invitato a condividere il materiale ufficiale già pubblicato dai canali Social dell'Organizzazione;
    h. avere sempre un comportamento pubblico rispettoso dell'Organizzazione presso cui lavora;
    i. è tenuto a formulare ogni intervento nel massimo rispetto degli altri, in particolare dei colleghi e della loro privacy e dei cittadini/utenti e dei portatori di interesse in generale.

j. I comportamenti non consentiti:
k. pubblicare contenuti irrispettosi verso il proprio responsabile o i propri colleghi;
l. pubblicare contenuti denigratori nei confronti di terzi, anche in via indiretta;
m. pubblicare contenuti dove possa apparire una opinione attribuibile all'Organizzazione;
n. utilizzare il logo dell'Organizzazione su account personali, specie se non approvato o deformato;
o. divulgare informazioni di qualsiasi natura, comunque riservate o interne all'Organizzazione (si rammenta a tal proposito che la clausola di riservatezza del codice di comportamento per il personale dipendente vale anche sui Social Media);
p. commentare in merito ad informazioni, eventi, fatti, situazioni inerenti all'Organizzazione (come sopra accennato, si ricorda che la gestione dei feedback negativi spetta soltanto al Responsabile dei social media);
q. aprire profilo, quali ad esempio blog, pagine o altri canali, legati all'Organizzazione senza specifica autorizzazione della Direzione;
r. attribuirsi ruoli non ufficiali senza specifica autorizzazione della Direzione;
s. pubblicare un commento dal profilo personale che contenga turpiloquio o volgarità.

Art. 19. - Gestione di una conference call (*Etiquette Rules*)

1) In una riunione tramite strumenti informatici valgono le stesse regole di educazione di una riunione convenzionale frontale. Vi sono però dei vincoli e dei possibili problemi legati alle tecnologie che richiedono una particolare attenzione al fine di evitare perdite di tempo e insoddisfazione dei partecipanti.
2) È importante concordare con congruo anticipo lo strumento e il momento preciso in cui tenere la call. L'organizzatore deve inviare un invito, verificando prima le agende condivise, in modo che sia possibile attivare semplicemente con un click lo strumento prescelto per la conferenza, senza sprechi di tempo e chiamate parallele del tipo "cosa utilizziamo per la call?";
3) La regola generale prescrive che chi ha bisogno cerca, invita e chiama; viceversa, chi fornisce il supporto deve essere chiamato da colui che ha bisogno;
4) Considerati gli strumenti, le modalità e gli immancabili disturbi e disconnessioni, la call dovrebbe essere di una durata pari a 10, 20 o al massimo di 30 minuti nei quali concentrare l'essenza dei contenuti della riunione. I materiali dovrebbero essere condivisi con congruo anticipo in modo che i partecipanti possano comunque apportare il loro contributo senza discussioni o perdite di tempo; le slides per le presentazioni NON devono essere condivise preliminarmente ma mostrate esclusivamente nella sessione;
5) Nel caso in cui un partecipante sappia in anticipo di un probabile ritardo, è tenuto a comunicarlo all'organizzatore in modo che, se possibile, la call venga fissata in un secondo momento o posticipata;
6) Data l'impossibilità di multitasking nelle call, quando un partecipante non risponde alle chiamate o agli inviti, non è corretto insistere o lasciare messaggi, almeno la prima volta. Se dopo diversi tentativi il soggetto non risponde, è opportuno lasciare un messaggio o inviare una e-mail. A meno di particolari urgenze, l'organizzatore non dovrebbe richiamare;
7) L'organizzatore dovrebbe invitare alla call il minor numero di persone possibile poiché più persone partecipano, più difficilmente verrà prestata la dovuta attenzione;
8) Tutti i partecipanti alla call devono prestare attenzione al luogo da dove viene effettuata la chiamata, ovvero in ambiente tranquillo, senza rumori di fondo e sempre supportati da una buona connettività (di solito il Wi-Fi in giardino non permette lo stesso livello di qualità audio e video); sono esclusi luoghi pubblici, in presenza di altre persone anche se familiari, specie nel caso di trattazione di temi dell'organizzazione, delicati o comunque sottoposti a segreto di ufficio;
9) Ad esclusione dell'organizzatore, tutti i partecipanti si accertano di tenere chiusa (in modalità mute) la comunicazione audio in modo da evitare rumori di fondo o effetti Larsen (feedback acustico o più

ritorno); il passaggio da muto a microfono attivo è effettuato dal partecipante solo in caso di richiesta di intervento o per richiedere la parola;

10) In caso di utilizzo di sistemi di comunicazione nuovi, non conosciuti, è opportuno accertarsi preliminarmente dei prerequisiti (installazione di applicazioni software, componenti, plug-in, livelli audio) ed effettuare almeno un test preliminare;
11) Nelle prime sessioni di conference è preferibile utilizzare la versione video con la ripresa delle persone sfruttando la possibilità di conoscersi se non se ne è avuta in precedenza occasione; per le versioni successive può essere consigliata la audio conference (senza video) con condivisione dei materiali;
12) A meno di particolari situazioni, la call deve iniziare e concludersi nei tempi stabiliti; non è corretto attendere indefinitamente i ritardatari soprattutto per non incoraggiare la loro condotta, pertanto, chi arriva in ritardo potrà essere contattato direttamente dall'organizzatore in modo da poter ricevere le informazioni perdute senza effetti negativi sugli altri partecipanti;
13) L'organizzatore della call deve mostrarsi immediatamente, presentare i partecipanti, esporre i contenuti e dare le dovute indicazioni di servizio, tra le quali il tempo previsto per la call ed i relativi interventi; i partecipanti devono venire a conoscenza sin da subito di ciò che l'organizzatore si aspetta da loro;
14) La modalità di comunicazione frontale e in call si differenzia altresì per la necessità di adottare un linguaggio più semplice, frasi concise e pause regolari tra i differenti contenuti. Questo consentirà ai partecipanti di passare oltre o in alternativa di porre delle congrue domande;
15) L'organizzatore della call deve prestare attenzione alla stessa partecipazione, intervenendo e togliendo la parola a chi prova a monopolizzare la sessione e chiamando gli altri ad intervenire;
16) Pur avendo a disposizione altri strumenti del sistema informatico o lo smartphone, non è corretto continuare a rispondere alle e-mail o ai messaggi mentre gli altri partecipano attivamente alla sessione; le altre attività devono essere posticipate dopo la call;
17) Prima della fine della sessione è necessario avvertire i partecipanti della imminente conclusione e della possibilità da quel momento di rivolgere opportune domande;
18) L'organizzatore della call, o un soggetto nominato segretario, deve annotare ed in seguito condividere il report della sessione:
    a. Motivo della call / obiettivi
    b. Nominativo e ruolo partecipanti
    c. Argomenti discussi e relativi interventi
    d. Risultanze

CAPO III – Attori e ruoli

Art. 20. - Utilizzatore dei servizi e degli applicativi

1) L'Utilizzatore dei servizi e degli applicativi è un individuo espressamente autorizzato ad effettuare trattamenti di dati attraverso applicazioni software. Le autorizzazioni possono essere nominali o per funzione ovvero per appartenenza a uno specifico gruppo di lavoro.
2) Le autorizzazioni sono concesse dal Dirigente dell'Area che individua ambito e profilo di autorizzazione con comunicazione ai Sistemi Informativi, che provvede alle necessarie impostazioni a livello di sistema o di applicativo.
3) L'Utilizzatore dei servizi e degli applicativi deve attenersi scrupolosamente alle procedure operative indicate nei manuali d'uso, nelle note operative, negli aiuti in linea, illustrati durante le sessioni formative o comunicate durante il cosiddetto *learning by doing (imparare facendo).*
4) Gli utilizzatori dei servizi e degli applicativi hanno l'obbligo di segnalare immediatamente al proprio Dirigente qualsiasi evento o situazione di rischio della sicurezza dei sistemi e delle reti di

comunicazione, al fine di tutelare il patrimonio informativo dell'organizzazione e garantire la necessaria continuità operativa.

Art. 21. - Amministratori di Sistema

1) Il personale sistemistico e di networking, avendo facoltà di accesso alle informazioni anche senza i vincoli e le protezioni del livello applicativo, è nominato Amministratore di Sistema dal Dirigente dei Sistemi Informativi o dal Dirigente dell'Area che provvede ad attribuire singolarmente l'ambito di autorizzazione. Sono considerati Amministratori di sistema i tecnici che lavorano a tutti i livelli della catena tecnologica al di sotto dello strato applicativo a meno che possano definire e rilasciare credenziali di autenticazione.
2) A partire dal livello "visibile", la catena tecnologica è composta da:
    a. Livello applicativo;
    b. Middleware (DBMS e web service);
    c. Sistemi operativi;
    d. Hypervisor;
    e. Server e sottosistemi SAN/NAS;
    f. Network.
3) I principali compiti di un Amministratore di Sistema sono i seguenti:
    a. Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
    b. Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
    c. Installare e configurare nuovo hardware/software sia lato client, sia lato server;
    d. Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'organizzazione;
    e. Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
    f. Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di *troubleshooting*;
    g. Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
    h. Documentare le operazioni effettuate (*Logbook*), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
    i. Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
    j. Operare secondo le prescrizioni di sicurezza e le procedure interne previste.

Art. 22. - Fornitori di prodotti e servizi

1) I fornitori di prodotti e servizi dei Sistemi Informativi sono coloro che provvedono all'approvvigionamento di beni o alla prestazione di servizi all'organizzazione. In fase di appalto, dichiarano di accettare le regole e le procedure del presente regolamento.
2) In caso di *outsourcing* di un servizio relativo a un sistema oppure ad un applicativo, il personale tecnico è nominato Amministratore di Sistema dal titolare dell'azienda appaltatrice, che nello specifico svolge il ruolo di Responsabile (esterno) del trattamento ai sensi dell'art. 28 del GDPR. Almeno una volta l'anno, il titolare dell'azienda appaltatrice comunica al Direttore dei Sistemi Informativi l'elenco degli Amministratori di Sistema nominati e autorizzati a effettuare il servizio relativo all'appalto.

Art. 23. - Data Protection Officer (DPO) o Responsabile della protezione dati personali

1) Il DPO ha le seguenti responsabilità (oltre a quanto già previsto dall'art. 39 del GDPR):
    a. Sensibilizzare e formare il personale in modo da garantire un adeguato livello di consapevolezza sulle minacce alla sicurezza informatica;
    b. Gestire le procedure di data breach;

c. Fungere da punto di contatto con l'Autorità Garante della protezione dei dati personali.

Glossario

VPN	Rete privata virtuale; modalità di collegamento sicuro alla rete dell'organizzazione
DMZ (zone demilitarizzate)	Sottorete isolata a livello fisico o logico nella quale sono pubblicati dei servizi informatici accessibili da LAN che da WAN
Hosting	Allocazione di un servizio o applicativo su un server pubblicato in Internet
Housing	Locazione di uno spazio fisico, generalmente all'interno di appositi armadi detti rack
Facility	Infrastrutture necessarie al funzionamento di un datacenter
Middleware	Software intermediari che permettono la comunicazione tra protocolli e sistemi operativi differenti
Wi-Fi	Rete wireless
BYOD	Bring your own device – dispositive personali utilizzati dai dipendenti per fruire di informazioni e applicazioni
instant messaging	Sistemi di comunicazione in tempo reale in rete
log	Sistema o modalità di registrazione degli eventi
Logbook	Contenitore dei log
keylogger	Malware in grado di registrare tutti i caratteri registrati da tastiera
firewall	Sistema di protezione dai pericoli della rete Internet
antispam	Sistema di filtraggio della posta indesiderata
phishing	Tipologia di attacco in cui si induce la vittima a fornire informazioni
forward	Re-invio automatico o manuale di un messaggio
CAD	Codice dell'Amministrazione Digitale
Smart card	Dispositivo hardware con potenzialità di elaborazione e memorizzazione dati in grado di garantire elevati standard di sicurezza
SDI	Sistema di Interscambio per la Fatturazione elettronica PA
device wipe-out	Modalità di cancellazione totale o parziale dei contenuti per motivi di sicurezza di un dispositivo in caso di perdita dello stesso
Content Filtering	Filtraggio della navigazione Internet in modo da evitare siti web non allineati con gli obiettivi dell'organizzazione
Hacking	Metodi, tecniche e operazioni volte a conoscere, accedere e modificare un sistema informatico
plug-in	Programma non autonomo che interagisce con un altro programma per ampliarne o estenderne le funzionalità originarie
packet shaping	Modalità di adattamento della comunicazione in base a politiche di miglioramento del servizio
criptazione	"offuscare" un messaggio o un documento in modo da non essere comprensibile/intelligibile alle persone non autorizzate
retention	Tempistiche di conservazione dei backup
IaaS, PaaS e SaaS	Rispettivamente infrastrutture, piattaforme e software erogabili *on demand* sul cloud
Social Engineering	Studio del comportamento individuale di una persona al fine di carpire informazioni utili.
Retraining	Ripetizione della formazione prevista per uno specifico argomento
troubleshooting	Processo di ricerca logica e sistematica delle cause di un problema su un prodotto o processo affinché possa essere risolto

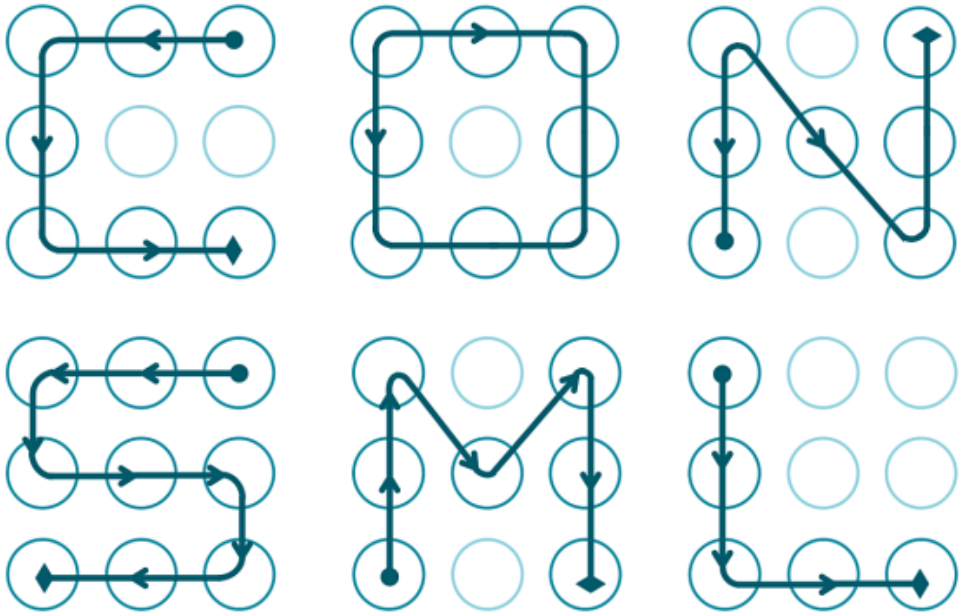
Appendice 1 - Password presenti nei dizionari pubblici

In ordine di frequenza rilevata:

Password	123456	123456789	Qwerty	password
1111111	12345678	abc123	1234567	1234567890
9876543210	password1	12345	letmein	football
iloveyou	admin	welcome	monkey	login
starwars	123123	dragon	passw0rd	master
hello	freedom	whatever	qazwsx	trustno1

Le password riportate in questo elenco NON DEVONO essere utilizzate.

Appendice 2 – Combinazioni "FACILI" di sblocco smartphone e tablet



Le combinazioni di sblocco riportate in questo elenco NON DEVONO essere utilizzate.

PIN più utilizzati (4 cifre)

1234	1111	0000	1212
7777	1004	2000	4444
2222	6969	9999	3333
5555	6666	1122	1313
8888	4321	2001	1010

I PIN riportati in questo elenco NON DEVONO essere utilizzati.

Appendice 3 – Categorie di *Content Filtering*

Le seguenti tipologie di siti web non sono navigabili con gli strumenti messi a disposizione dell'organizzazione:

- Adult / Mature Content
- Bandwidth Consuming
- General Interest – Business
- Potentially Liable
- Security Risk

Approvato dal Consiglio d'Istituto il 27/06/2025