Regolamento per l'utilizzo di dotazioni e strumenti informatici della CSEA

Sommario

REGISTRO DELLE MODIFICHE

Versione e Stato del documento	Attività svolta	Data	Modificato da	Ulteriori attività necessarie
Versione 1 Bozza	Prima redazione del documento del 2022	25/2 – 8/3	Fabrizio Usai	Integrazioni per includere di Compliance e di Certificazioni ISO/IEC.
Versione 1.1 Bozza	Revisione per la parte di Compliance	8/3	Flavio Tuosto	Revisione per la parte di Certificazioni ISO/IEC
Versione 2.0 Verificato	Revisione collegiale	11/3	Gianluca Ritarossi, Flavio Tuosto, Pietro Abbati Marescotti	Revisione finale per approvazione ASI
Versione 2.1 Approvato ASI	Revisione	11/3	Pietro Abbati Marescotti	Revisione Team Privacy e PE
Versione 2.2 Revisionato	Revisione PE	14/3	Revisione effettuata da Cristina Terracciano; ulteriori modifiche apportate da Pietro Abbati Marescotti	Revisione ufficio Team Privacy
Versione 2.3 Definitivo	Revisione Team Privacy	14/3	Pietro Abbati Marescotti (su base mail ricevuta dal Team Privacy)	Revisione DPO
Versione 2.4 Revisionato	Revisione DPO	20/3	DPO (nome file ricevuto “rev_FCOLORI”)	ASI: valutazione delle proposte della DPO
Versione 2.5 Revisionato	Revisione ASI	21/3	ASI	CSEA collegialmente: valutazione delle proposte della DPO
Versione 2.6 Approvato CSEA	Revisione congiunta ASI – LCS - PE – Privacy	28/3	ASI Pietro Abbati Marescotti	Consegna definitiva
Versione 2.7 Revisionato Team Privacy	Riscontri team Privacy	12/4	Team Privacy	Integrare le revisioni proposte (riformulazione di un capoverso)

Versione 2.8	Integrazioni minori (riformulazione di un capoverso) delle proposte del team Privacy	3/5	Pietro Abbati Marescotti (su base mail ricevuta dal Team Privacy)	
Versione 2.9	Revisione del documento per migliore formattazione ed errori di battitura		Pietro Abbati Marescotti	
Versione 2.10	Revisione dell'esempio di password a piè di pagina		Pietro Abbati Marescotti	Revisione da parte del DG
Versione 2.11	Revisione del documento per nuova struttura organizzativa		Cristina Terracciano	Ultima lettura per condivisione revisioni e definizione documento finale
Versione 2.12	Revisione "misure minime di sicurezza ICT"		Flavio Tuosto	Condivisione e raccolta revisioni e definizione documento finale

Definizioni ed acronimi

Definizioni ed Acronimi	Descrizione
Antivirus	Software specializzato per la ricerca e l'eliminazione dei virus e dei malware
BIOS	Il Basic Input-Output System (in acronimo, BIOS), in informatica, è il primo programma che viene eseguito dopo l'accensione, coinvolto pertanto nella fase di avvio del sistema di elaborazione.
Bridging	Connessione tra segmenti di rete
Browser	Software installato sulla postazione di lavoro degli utenti che consente loro l'accesso alle pagine Web su Intranet ed Internet
Cache	Memoria temporanea delle pagine visitate
CD – DVD	Supporti di memorizzazione ottica
Chiavi USB	Dispositivi di memoria esterna accessibili via USB
Client di posta elettronica	Software per la gestione della posta elettronica installato sulla postazione di lavoro dell'utente e da lui utilizzato per accedere al servizio di posta elettronica
ASI	Area Sistemi Informativi
Firewall	Dispositivo hardware o software che protegge una rete da accessi non autorizzati, fornendo un unico punto di accesso da e verso l'esterno. Questo dispositivo di sicurezza è dotato di funzionalità di filtro, registrazione e controllo del traffico dei dati in ingresso ed in uscita dalla rete.
Garante	Garante per la protezione dei dati personali
Hacking	Tecniche di aggiramento delle protezioni di sicurezza informatica
Help Desk	Funzione di ASI per l'assistenza agli utenti
CSEA	Cassa per i servizi energetici e ambientali
Ente	CSEA
LOG	File o archivio informatico contenente la traccia degli eventi, sistemistici o applicativi, rilevati da parte dei sistemi informatici
Log	File contenenti registrazioni delle attività
Mailbox	Casella di posta
Mail server	Sistema centralizzato di posta elettronica
Malware	Software che si auto-installa sul computer e che può alterare il normale comportamento del computer e, all'insaputa dell'utente, può raccogliere informazioni dal computer e trasmetterle all'esterno (Virus, Spyware, rootkit, ecc..)
Modem	Dispositivo elettronico per i collegamenti via doppino telefonico
PdL	Postazione di lavoro (workstation, laptop, desktop, notebook, smartphone, ecc..)
Phishing	Comunicazioni fraudolente volte a carpire informazioni riservate
Regolamento	Il presente "Regolamento per l'utilizzo di dotazioni e strumenti informatici della CSEA". Si precisa che ai fini della disciplina dello *smart working* ordinario, il presente Regolamento viene definito "*Disciplinare sull'utilizzo degli strumenti informatici*"

Proxy	Il proxy è un dispositivo centralizzato che consente la connessione alla rete Internet da parte di tutti i computer della rete Intranet, controllando i diritti di accesso e applicando le regole di URL filtering
Screensaver	Software che visualizza sul monitor un'immagine e ne blocca l'accesso quando il computer non viene utilizzato per un determinato periodo di tempo
Spamming	Mail massive e indesiderate
SPC	Sistema Pubblico di Connettività
SSL	Secure Socket Layer. Protocollo di sicurezza che assicura transazioni sicure in Internet attraverso un sistema di cifratura
Trojan horses	Cavallo di troia: tipologia di malware (software malevolo)
Tunneling	Tecnica di trasmissione di dati privati attraverso Internet
URL Filtering	Meccanismo di controllo che impedisce l'accesso ad alcuni siti internet notoriamente contenenti materiale non consentito dalle politiche istituzionali
USB	Universal Serial Bus: dispositivo di accesso dei personal computer
Utente	Persona, interna o esterna, che utilizza il sistema informatico di CSEA
Virus	Tipologia di malware (software malevolo)
VPN	Virtual Private Network
Wireless	Sistema di accesso ad Internet via onde radio a breve distanza

Premessa

Il Garante per la protezione dei dati personali raccomanda l'adozione da parte dei datori di lavoro pubblici e privati di un **Regolamento interno**, nel rispetto della Legge 20.05.1970, n. 300 (Statuto dei lavoratori), del Regolamento (UE) n. 2016/679 (GDPR) e del Decreto Legislativo 30.06.2003, n. 196 e s.m.i. (Codice in materia di protezione dei dati personali), Legge 13.12.1993 n. 547 (Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica), Legge 18.08.2000 n. 248 e s.m.i. (Tutela del diritto di autore).

Con il presente Regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche che la CSEA mette a disposizione del personale dipendente e non dipendente per l'esecuzione dei propri compiti lavorativi di competenza, al fine di tutelare il patrimonio informativo dello stesso.

Sono definite le raccomandazioni generali e le regole comportamentali cui devono attenersi gli utenti, al fine di garantire l'utilizzo in sicurezza dei servizi informatici e degli strumenti in coerenza con la politica della CSEA e con le norme di legge attualmente in vigore.

I contenuti di questo documento si applicano a tutti i dipendenti della CSEA e, in generale, a tutti coloro che, in virtù di un rapporto di lavoro o fornitura (per esempio, consulenti, fornitori, stagisti, risorse in somministrazione di seguito denominati utenti esterni), gestiscono ed utilizzano gli strumenti informatici forniti dalla CSEA.

Ogni nuovo contratto di fornitura di servizi dovrà richiedere l'osservanza delle disposizioni enunciate nel presente documento.

È responsabilità del referente di Divisione/Direzione, Area, Ufficio, di ogni altra figura apicale nonché dei responsabili della conduzione di contratti, in cui sono previsti accessi ai sistemi informatici e/o telefonici della CSEA, informare tutti i soggetti interessati dell'esistenza del presente Regolamento, nonché far adottare e sovrintendere alla sua corretta applicazione.

Il presente Regolamento è stato redatto sulla base delle linee guida contenute nel provvedimento del Garante *Privacy* "**Lavoro: le linee guida del Garante per posta elettronica e internet"** pubblicato su Gazzetta Ufficiale n. 58 del 10 marzo 2007 ed è pertanto indispensabile la sua conoscenza da parte di tutti i dipendenti e collaboratori.

L'utente è personalmente responsabile del rispetto del presente Regolamento. Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento, può comportare responsabilità civili, penali e amministrative (sia per la CSEA sia per il singolo dipendente) ed è perseguibile anche con provvedimenti disciplinari.

È, pertanto, essenziale che tutti i dipendenti e collaboratori della CSEA conoscano la legislazione vigente e siano consapevoli della necessità di rispettare i principi generali di correttezza, lealtà e buona fede che regolano il rapporto con la CSEA, nonché il Codice Etico della CSEA. A tal proposito, si riportano nel successivo

paragrafo, a titolo meramente esemplificativo e non esaustivo, alcuni dei principi e delle disposizioni più significative in materia.

Riferimenti Normativi e documentali

NORMATIVA EUROPEA

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati personali" o "GDPR").

Principi applicabili al trattamento di dati personali (Art 5, par. 1, del GDPR)

a) Liceità correttezza e trasparenza: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
b) Limitazione della finalità: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
c) Minimizzazione dei dati: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
d) Esattezza: i dati personali sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
e) Limitazione della conservazione: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
f) Integrità e riservatezza: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Sicurezza del trattamento (Art. 32, par. 1 del GDPR)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

NORMATIVA ITALIANA

- Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni ("Codice in materia di protezione dei dati personali").

- Legge 20 maggio 1970, n. 300 e successive integrazioni e modificazioni, recante “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento” (“Statuto dei Lavoratori”).
- Decreto Legislativo 8 giugno 2001, n. 231, recante la “Disciplina della responsabilità amministrativa delle persone giuridiche, delle Aziende e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della legge 29 settembre 2000, n. 300”, pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.
- Articolo 23 del Decreto Legislativo n. 151/2015 (c.d. Jobs Act) integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell’attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell’attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».
- Decreto Legislativo 29 dicembre 1992 n. 518 Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore.
- Legge 22 aprile 1941 n. 633 s.m.i. sulla tutela del diritto d’autore.
- Legge 13.12.1993 n. 547 (Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica)
- Legge 18 agosto 2000 n. 248 s.m.i. (Tutela del diritto di autore).

Codice civile

- Art. 2049: Responsabilità indiretta dell’imprenditore;
- Art. 2086: Direzione e gerarchia nell’impresa;
- Art. 2087: Tutela dell’integrità fisica e della personalità morale dei dipendenti, da parte dell’imprenditore;
- Art. 2104: Diligenza del dipendente nel rispetto delle disposizioni impartite dall’imprenditore.

PROVVEDIMENTI AUTORITA’ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Linee Guida del Garante Privacy su Posta Elettronica e Internet (doc. web n. 1387522 - Deliberazione n. 13 del 1° marzo 2007 – G.U. n. 58 del 10 marzo 2007);
- Provvedimento relativo al “Trattamento di dati personali effettuato sugli account di posta elettronica aziendale” - 1° febbraio 2018” n. 53 (doc. web n.8159221)

AGENZIA PER L’ITALIA DIGITALE - AGID

- Circolare dell’Agenzia per l’Italia Digitale – AGID n. 2 del 18 aprile 2017 relativo a “Misure minime di sicurezza ICT per le pubbliche amministrazioni”.

Ruoli e responsabilità

Area Sistemi Informativi

L’Area Sistemi Informativi (ASI) è Responsabile della definizione degli aspetti di sicurezza tecnico-organizzativi inerenti ai servizi informatici della CSEA e quindi definisce, con le altre strutture competenti, le procedure organizzative e/o operative che regolamentano i servizi informatici della CSEA.

In particolare, ASI è Responsabile:

- di definire le politiche di URL Filtering, identificando le categorie di siti Internet il cui accesso sarà bloccato in quanto contrari alla legge, all'ordine pubblico, al buon costume, all'etica della CSEA, nonché di contenuto oltraggioso o discriminatorio;
- di analizzare, in forma aggregata ed anonima, i log di sicurezza e di individuare le possibili contromisure per risolvere eventuali minacce alla sicurezza;
- di stabilire il limite massimo dello spazio riservato alle caselle di posta elettronica sul server e le dimensioni massime consentite per i messaggi inviati e ricevuti;
- di provvedere all'attività di installazione ed attivazione di software antivirus o di analisi di comportamenti anomali a protezione delle Postazioni di lavoro degli utenti;
- di definire i processi di creazione, abilitazione, modifica, disattivazione, ripristino e cessazione degli account di accesso ai servizi informatici, dietro esplicita e specifica richiesta pervenuta

ASI è il punto di contatto per la gestione degli incidenti informatici e, più in generale, degli utilizzi non corretti degli strumenti correlati e delle violazioni informatiche, fermo restando il rispetto di quanto previsto dalla "*Procedura per la gestione e la notifica del data breach*" vigente.

ASI riceve, analizza e gestisce le segnalazioni ricevute dagli utenti, per sospette violazioni di sicurezza ed è contattabile tramite il sistema Gestione Progetti nell'area dedicata allo scopo denominata "Sicurezza Informatica e Compliance" (https://gestioneprogetti.csea.it/projects/sicurezza-informatica-e-compliance/issues). In caso di particolare criticità o urgenza esclusivamente per temi di sicurezza informatica gli utenti dovranno contattare anche telefonicamente gli Amministratori di Sistema.

Inoltre, agli Amministratori di Sistema dell'Ente sono assegnati i compiti di seguito riportati:

- proporre al Direttore generale modifiche al Regolamento in caso di variazioni normative e/o relative all'organizzazione della CSEA;
- al fine di garantire la corretta attuazione del Regolamento, porre in essere tutte le misure operative e proporre al Direttore generale l'adozione di eventuali procedure ritenute necessarie;
- notificare al Direttore generale eventuali violazioni del Regolamento.

Responsabili di Divisione/Direzione, Area, Ufficio e di esecuzione dei contratti

I Responsabili sono tenuti alla distribuzione, sensibilizzazione e verifica dell'applicazione del presente Regolamento. Rimane fermo quanto già espresso in merito nell'introduzione del presente documento.

È responsabilità del referente di Divisione/Direzione, Area, Ufficio, di ogni altra figura apicale nonché dei responsabili della conduzione di contratti in cui sono previsti accessi ai sistemi informatici e/o telefonici della CSEA di notificare a tutti i soggetti interessati il presente Regolamento, di farlo adottare nonché di sovrintendere alla sua corretta applicazione.

Utente

L'utente è personalmente responsabile in particolare, oltre che della piena osservanza del presente Regolamento:

- delle credenziali a lui assegnate, sia per la loro generazione in conformità con le indicazioni di ASI che della loro custodia e non divulgazione;
- di tutte le attività che svolge attraverso l'utilizzo degli strumenti informatici e/o telefonici;
- della pronta comunicazione di difformità da parte propria o dei colleghi rispetto a quanto previsto dal presente Regolamento;
- della massima attenzione a tutti i temi di Sicurezza Informatica qui indicati e/o comunicati in itinere da ASI.

Rimane fermo quanto già indicato nella premessa relativamente al mancato rispetto o la violazione delle regole contenute nel presente Regolamento.

Procedure di Supporto e Contatto

In ASI è attiva la funzione di supporto contattabile tramite il sistema Gestione Progetti (https://gestioneprogetti.csea.it) che eroga servizi di assistenza agli utenti, fornisce informazioni sulle modalità di utilizzo di un prodotto o servizio, aiuta gli utenti nella risoluzione di problemi tecnici, monitora e risolve i problemi o le eventuali violazioni di sicurezza che potrebbero emergere nello svolgimento delle attività lavorative.

Per i soli casi di impossibilità a contattare il servizio di supporto tramite il sistema Gestione Progetti sarà possibile contattare i referenti di helpdesk.

Utilizzo della Postazione di lavoro

Gli utenti sono tenuti a:

- adottare politiche di "scrivania pulita" e "schermo pulito", rispettivamente per i documenti ed i supporti di memorizzazione delle informazioni ed i sistemi/servizi di elaborazione delle informazioni;
- chiudere a chiave le informazioni di business critiche riportate su carta o su supporti di memorizzazione digitale, quando non utilizzate, soprattutto quando la postazione di lavoro è vuota;
- non lasciare collegati computer e terminali o proteggerli, quando non in uso e incustoditi, con un salva-schermo e meccanismi di blocco della tastiera controllati con una password o con altri meccanismi similari di autenticazione, e tramite lucchetti con chiave, password od altri controlli.

Utilizzo Strumenti Informatici

Gestione dei privilegi di accesso ai sistemi e delle password

- L'accesso alla rete ed ai servizi di business erogati dai programmi (software) aziendali sono consentiti attraverso l'autenticazione composta da un nome utente ed una password segreta, oltre all'autenticazione a più fattori. Le autenticazioni di accesso ai servizi di rete sono amministrate da Microsoft Active Directory che consente autenticazioni crittografate. La gestione dei privilegi di accesso ai servizi applicativi diversi da quelli amministrati direttamente da Microsoft Active Directory è implementata nelle soluzioni legacy della CSEA.
- Le autorizzazioni di accesso ai servizi erogati dalle applicazioni interne e dai servizi di rete della CSEA sono assegnate a fronte di specifiche richieste dei responsabili delle unità organizzative.
- L'assegnazione delle autorizzazioni di accesso ai servizi erogati avviene attraverso richiesta formale tramite piattaforma Gestione Progetti, che viene presa in carico previa verifica dell'effettiva esigenza di accesso/recesso al servizio in oggetto.
- La password di autenticazione associata a ciascun utente deve essere di rilevante complessità. Essa, peraltro, non deve assolutamente contenere riferimenti agevolmente riconducibili all'incaricato; è quindi vietato l'utilizzo di password consistenti nel nome (o cognome) dell'incaricato stesso, nella sua data di nascita, nel nome dei familiari, della sua città, della squadra del cuore et similia.
- La password viene inizialmente stabilita dall'Amministratore di Sistema e deve essere immediatamente sostituita dall'utente al primo accesso e custodita con la massima diligenza sin dal primo utilizzo.
- Si ricordi, peraltro, che la password deve essere:
    - privata: conosciuta ed utilizzata unicamente da un soggetto;
    - segreta: essa non deve apparire "in chiaro", né in un file né sul cellulare o su biglietti attaccati sul terminale del PC;
    - non divulgata (nemmeno ai colleghi o al proprio Responsabile);
    - non trascritta o custodita in posti insicuri;
    - non digitata davanti ad altri (assicurarsi sempre di non essere osservati durante l'inserimento delle credenziali per accedere ai sistemi);
    - non memorizzata, in associazione allo userid, sul PC;
    - elaborata attraverso un compromesso tra complessità e facilità nella memorizzazione: è necessario evitare, in tal modo, l'opportunità di doverla scrivere in un documento non riservato;
    - risultante da una combinazione di lettere maiuscole, minuscole e segni d'interpunzione o, quanto meno, una stringa di caratteri alfanumerici, una breve frase, una parola non presente sui dizionari, nemmeno se esteri (es.: comP!!UTer1234FG...) e sempre diversa

dalle precedenti[1], composta da almeno 9 caratteri comprendenti maiuscole, minuscole, numeri e segni di punteggiatura o caratteri speciali (es. #°§^[ç);
    - sostituita all'occorrenza o almeno ogni 90 giorni, selezionando la nuova password in modo tale che a) siano utilizzati almeno quattro caratteri diversi rispetto alla password precedente e b) senza replicare le ultime 5 password.
- Al fine di garantire nel tempo un accurato controllo degli accessi è previsto, a cura dell'Amministratore di Sistema e con frequenza almeno annuale, un riesame delle autorizzazioni di autenticazione alla rete ed ai servizi di business erogati dai software aziendali. L'attività di riesame prevede la bonifica di ogni anomalia riscontrata da tale confronto.
- Non è consentito riutilizzare le credenziali di accesso ai sistemi informatici aziendali per l'autenticazione a servizi informatici non attinenti all'attività lavorativa quali, ad esempio, caselle di posta personali, Social Network, Forum, ecc.

Utilizzo Personal Computer

- Il Personal Computer affidato al dipendente e/o al collaboratore è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa e/o per finalità estranee al rapporto di lavoro è pertanto vietato, in quanto esso può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
- L'accesso ai suddetti dispositivi deve essere protetto da credenziali di autenticazione (es. caratteristiche biometriche, PIN o credenziali mnemoniche, quali user ID e password et similia) che devono essere custodite dall'incaricato con la massima diligenza e riservatezza, mantenute segrete e non comunicate o diffuse per alcuna ragione.
- Non è consentita l'attivazione della password né la modifica del bios, senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
- L'Amministratore di Sistema ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno (ivi compresi gli archivi di posta elettronica) e/o agli strumenti utilizzati, in particolare in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per assicurare l'operatività, la sicurezza del sistema e il normale svolgimento dell'attività aziendale, informando tempestivamente l'incaricato dell'accesso posto in essere.
- Il Personal Computer deve essere:
    - spento ogni sera prima di lasciare la postazione di lavoro, o in caso di assenze prolungate dalla stessa;
    - sospeso (mediante attivazione di blocco) ogni volta che la postazione di lavoro viene lasciata; il successivo accesso all'elaboratore dovrà avvenire a mezzo di autenticazione.
- È noto che lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso. Ove sorgesse l'esigenza di

[1] Un pratico metodo è inserire parti di copertine o libri disponibili in casa. Prendendo ad esempio questa copertina:  la relativa scritta  "n.3286 €2,70* TANTI AUGURI MICKEY!" rappresenta una password sicura ma comunque di facile memorizzazione

assentarsi dalla propria postazione di lavoro (anche per breve lasso di tempo), dovrà essere attivato in ogni caso il blocco dello schermo ed effettuata la disconnessione dalla rete (si suggerisce inoltre di spegnere il modem, ove possibile).

- Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione personale e non aziendale, di comunicazione o altro (ad esempio: masterizzatori, modem, USB disk drive, chiavette USB ecc.), se non previa espressa autorizzazione di ASI, dietro puntuale richiesta motivata. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus e/o malware.
- È fatto divieto di utilizzo di qualsiasi apparecchiatura che memorizzi ed elabori informazioni di proprietà della CSEA se non tramite gli stessi apparati messi a disposizione dall'Ente o, comunque, per i quali ci sia stata espressa deroga scritta.

In aggiunta, per quanto riguarda le cautele ulteriori da osservare nel caso di utilizzo di notebook (c.d. "PC portatile"), si specifica quanto segue:

- l'utente è responsabile del notebook assegnatogli dalla CSEA e deve custodirlo con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
- Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file presenti sugli stessi prima della riconsegna.
- I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.
- Se l'utilizzo del PC portatile (o, più in generale, di ogni ulteriore dispositivo) è condiviso da più utenti, la responsabilità del PC è da considerarsi attribuita al Responsabile dell'ufficio di competenza.
- Occorre prestare attenzione a non lasciare mai incustodito lo strumento in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici).
- Durante le missioni di lavoro il PC portatile deve essere portato come bagaglio a mano, evitando di trasportare nella medesima borsa i codici identificativi e le parole chiave di sicurezza (che, ripetiamo, dovranno essere conservati esclusivamente mnemonicamente) nonché i supporti di memorizzazione con le copie di back-up.
- È vietato lasciare incustodito sul mezzo di trasporto (es. autovettura, mezzo pubblico, treno, ecc.) lo strumento aziendale, anche se per soste brevi, indipendentemente dalla visibilità o meno dello strumento stesso dall'esterno.

Installazione non autorizzata di software

- Tutte le installazioni e le modifiche di configurazione del software devono essere effettuate da ASI; non è consentito installare autonomamente programmi o *app*, salvo previa autorizzazione esplicita di ASI, in quanto sussiste il concreto pericolo che gli stessi possano contenere spyware, adware o virus informatici tali da alterare la stabilità delle applicazioni dell'elaboratore o addirittura

danneggiare il sistema informatico aziendale. Ciò rimane valido anche per fonti considerate autorevoli.

- È inoltre vietato l'uso di programmi/software o app diversi da quelli distribuiti ed installati ufficialmente dall'Ente. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la CSEA anche a responsabilità civile e/o penale, in caso di violazioni della normativa a tutela del diritto d'autore (D.lgs. n. 518/92 in materia di tutela giuridica del software e L. n. 633/41 e s.m.i. in materia di tutela del diritto d'autore che impone la presenza, nel sistema, di software regolarmente licenziato o freeware).
- Non è consentito all'utente modificare le caratteristiche impostate sui propri asset in dotazione, oltre a basilari aspetti grafici già previsti dal sistema assegnato.
- I programmi messi a disposizione dalla CSEA non possono essere copiati in aree di memorizzazione diverse (dischi fissi, di rete o supporti e dispositivi mobili) da quelle in cui sono installati, salvo espressa autorizzazione e/o indicazione da parte di ASI.
- Non è consentito il trasferimento a terzi e la duplicazione, anche su elaboratori della CSEA, di programmi software dei quali la stessa sia titolare di licenza d'uso.
- L'Ente si riserva il diritto di effettuare controlli sulle configurazioni dei sistemi e sui programmi contenuti nei dischi fissi e di rete assegnati, anche eventualmente avvalendosi di tools automatizzati. Copie e configurazioni non autorizzate saranno rimosse, salva l'applicazione di ulteriori provvedimenti.

Utilizzo dei supporti ottici e magnetici

- Sono vietati l'installazione e l'utilizzo di dispositivi (quali, a titolo esemplificativo: chiavi USB, hard disk, dispositivi mobili, ecc.), se non previa specifica autorizzazione scritta di ASI dietro apposita richiesta motivata dell'utente, in quanto si tratta di operazioni che aumentano sensibilmente i rischi informatici.
- L'utilizzo e la copia di dati su supporti removibili di qualsiasi genere (es.: cd rom, HD esterni, chiavi USB, ecc.) non sono consentiti, salvo nei casi in cui ciò non sia strettamente necessario in ragione di effettive ed esclusive esigenze di servizio, comunque, previa autorizzazione del Responsabile di riferimento e limitatamente all'utilizzo di supporti di memorizzazione forniti dalla CSEA. L'utilizzo autorizzato di supporti di memorizzazione esterna implica la possibilità per la CSEA di verificarne il contenuto per finalità di sicurezza dei sistemi informativi.
- Tutti i supporti ottici e magnetici riutilizzabili (cassette di backup a nastro, chiavi USB, HD Drive) contenenti dati sensibili devono essere trattati con particolare cautela, anche in fase di smaltimento, onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la cancellazione e, addirittura, anche dopo la formattazione del supporto stesso.
- I supporti ottici o magnetici, utilizzabili singolarmente o contenuti nei dispositivi in dotazione (es. hard-disk del portatile), dovranno essere trattati con cura, lontano da fonti di calore e campi elettromagnetici che ne possano comprometterne l'integrità. Si raccomanda, inoltre, di osservare le istruzioni del produttore per la protezione delle apparecchiature.

- È proibito l'utilizzo di supporti ottici e magnetici per finalità diverse dallo svolgimento dell'attività lavorativa prevista.
- Si raccomanda per quanto possibile una limitazione e comunque particolare cautela nell'utilizzo dei suddetti dispositivi in quanto potrebbero veicolare infezioni informatiche o creare le condizioni per accessi indesiderati ai sistemi.
- Sui personal computer aziendali è attivo un sistema per la supervisione del corretto utilizzo dei sopracitati supporti di memorizzazione. L'adozione di tale sistema è finalizzata a ridurre i rischi per la sicurezza del patrimonio informativo aziendale quali, ad esempio, l'installazione non autorizzata di programmi e la propagazione di virus causati dall'improprio utilizzo di periferiche esterne.

Gestione dei Documenti Informatici

- Non sono consentiti, in ogni caso, né il trattamento né la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione ed inclinazione o appartenenza sindacale e/o politica. È parimenti vietata la visione e/o l'archiviazione di immagini o di contenuti multimediali a carattere osceno, riservati ad un pubblico adulto o comunque tali da offendere il comune senso del pudore.
- Non è consentito copiare o trasferire a terzi documenti elettronici (né tramite supporti di memorizzazione, né in via telematica) oltre i casi in cui l'attività sia condizione necessaria per lo svolgimento dell'attività lavorativa. Eventuali eccezioni dovranno essere sottoposte a previa esplicita autorizzazione del Responsabile di Divisione/Direzione, Area o Ufficio. Non sono consentiti né il trattamento né la memorizzazione di documenti elettronici o altro materiale informatico il cui contenuto non sia attinente all'attività lavorativa. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato/memorizzato, nemmeno per brevi periodi, nei sistemi informatici aziendali. Si evidenzia, peraltro, che sui sistemi vengono svolte regolari attività di monitoraggio, amministrazione e back-up. Potranno essere attivate regole automatiche in proposito limitando alcuni accessi per ottimizzarne l'uso. L'Ente si riserva di attuare ogni opportuna azione (ivi compresa eventualmente la cancellazione) in caso di rinvenimento di materiale la cui detenzione non sia legittima o sia non conforme a tale policy.
- Non è consentito il download/upload di file se non strettamente attinenti all'attività lavorativa e appartenenti a fonti/destinazioni affidabili. Nel caso in cui fosse necessario eseguire il download/upload di file di dimensioni superiori a 5GB, deve essere preventivamente avvisato il servizio di Help Desk al fine di verificare che questo non abbia impatti sulla performance della rete aziendale.
- Non è consentita la produzione di documenti informatici falsi, sia privati, sia pubblici, aventi efficacia probatoria.
- È responsabilità della CSEA identificare al proprio interno i soggetti abilitati all'accesso ai sistemi informativi atti alla comunicazione di dati alla Pubblica Amministrazione, con credenziali di accesso dedicate.
- Non è consentito memorizzare e/o trasferire dati della CSEA tramite servizi online di archiviazione/condivisione non già espressamente autorizzati da ASI, salvo diversa ed esplicita autorizzazione della CSEA. Al momento dell'adozione del presente Regolamento l'unico servizio online autorizzato per archiviazione e condivisione è Microsoft One Drive.

L'Ente rende noto che ASI è autorizzata a compiere interventi sui personal computer e dispositivi assegnati ai dipendenti, al fine di garantire la piena efficienza e la continuità delle attività, la sicurezza e la salvaguardia della rete aziendale, nonché per motivi tecnici quali ad esempio aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware.
Gli interventi potranno anche comportare l'accesso ai dati e alle informazioni trattate dal dipendente, ivi compresi quelli contenuti negli archivi di posta elettronica aziendale e sarà possibile in qualunque momento procedere alla rimozione di ogni file o applicazione che sia ritenuta pericolosa per la sicurezza della CSEA.

Telefonia fissa

Come disciplinato dalla vigente normativa e tenuto conto delle più recenti sentenze in materia della Corte di Cassazione, oltre che dei provvedimenti del Garante Privacy, la CSEA informa che i numeri di telefono in entrata ed in uscita dal centralino aziendale possono essere registrati per ragioni di sicurezza e controllo dei costi aziendali.

Le registrazioni dei numeri chiamanti e chiamati potranno essere conservate per un periodo non inferiore a sei mesi, in modo da consentire gli opportuni controlli dopo il ricevimento delle bollette da parte dei fornitori di servizi interessati.

Le registrazioni non verranno utilizzate con lo scopo di sanzionare i dipendenti ma per consentire invece un corretto utilizzo degli strumenti messi a disposizione degli stessi dalla CSEA. In caso di anomalie, queste verranno segnalate attraverso i Responsabili della CSEA al personale interessato. Comportamenti ripetuti e reiterati a seguito di segnalazioni di anomalie verranno gestiti come previsto dalla vigente normativa in materia di sanzioni disciplinari.

Dispositivi mobili (cellulari, tablet)

I telefoni e dispositivi mobili (tablet, smartphone ecc.), possono essere dotati di accesso ad Internet e costituiscono uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.

I dispositivi digitali mobili aziendali possono esser utilizzati anche ad uso personale alle seguenti condizioni:

- non devono essere generati costi a carico della CSEA;
- la connessione dati via rete mobile non deve essere utilizzata per "streaming video" e/o "peer to peer" o per altre attività ad elevato traffico dati;
- nei casi in cui il dipendente si trovi al di fuori dell'Italia, quest'ultimo dovrà anticipatamente, o comunque prontamente, comunicare ad ASI la necessità di utilizzo del dispositivo all'estero per finalità lavorative (reperibilità o attività lavorativa) per consentire una adeguata adozione di accorgimenti finalizzati al contenimento dei costi a carico dell'Ente;
- l'utilizzo dei suddetti dispositivi non deve interferire con le attività lavorative e comunque non deve essere in contrasto con le finalità e gli interessi della CSEA, dei suoi dipendenti, dirigenti, responsabili ed amministratori;

- in relazione all'utilizzo dei dispositivi sopra citati devono essere mantenute tutte le ulteriori indicazioni di sicurezza riportate nel presente Regolamento.

Si applicano, quindi, ai dispositivi digitali mobili aziendali, con le opportune declinazioni del caso (es "app" invece di "programmi") quanto già definito per l'utilizzo dei Personal Computer, siano essi portatili e non.

Non è consentita la manomissione/rimozione di eventuali meccanismi di sicurezza impostati dalla CSEA o dal produttore sul dispositivo.

Per consentire un'adeguata protezione delle informazioni aziendali, su alcuni dispositivi mobili in dotazione ai dipendenti potranno essere installate applicazioni (es. Mobile Device Management o Mobile Application Management) che possono acquisire ed elaborare informazioni sul loro utilizzo (es. configurazioni dei device, installazione/disinstallazione applicazioni, lista applicazioni, sincronizzazione) e consentire il loro blocco o la cancellazione a distanza delle informazioni (remote wiping).

Dispositivi e meccanismi di firma digitale

È fatto assoluto divieto di cedere, anche temporaneamente, le credenziali di firma digitale ad un altro soggetto. Per i casi opportuni si suggerisce, sussistendone le condizioni, di adottare lo strumento della delega.

Uso della posta elettronica, ordinaria e certificata

L'account di posta elettronica aziendale, pur avendo carattere personale in quanto caratterizzato da username riferibile al lavoratore, non potrà essere considerato di esclusiva appartenenza dello stesso. La casella di posta è un bene aziendale che costituisce uno strumento di lavoro, fornito dalla CSEA al lavoratore per consentirgli di svolgere al meglio le sue mansioni. Attraverso la mail aziendale gli utenti rappresentano pubblicamente l'Ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professione e comunque tale da riflettere l'immagine aziendale. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e prendono atto del fatto che è possibile un accesso alle stesse e ai messaggi ivi contenuti nei casi previsti per legge.

All'utente del servizio di posta elettronica è richiesto di attenersi alle seguenti indicazioni:

- utilizzare esclusivamente il *client* di posta elettronica *standard* messo a disposizione dalla CSEA (Outlook) o utilizzare l'accesso web allo stesso sistema secondo le modalità previste dalla CSEA;
- verificare periodicamente che il software antivirus sia correttamente installato, attivo e periodicamente aggiornato;
- segnalare tempestivamente la ricezione di messaggi che presentano un contenuto sospetto, potenzialmente pericoloso per l'integrità della postazione di lavoro, e notificare l'evento ad ASI;
- prestare la massima attenzione all'invio o alla ricezione tramite posta elettronica esterna di documenti di lavoro riservati in quanto potrebbero essere intercettati da terzi. Si ricorda che, salvo l'utilizzo da parte dell'utente di appositi strumenti di cifratura messi a disposizione dalla CSEA, i sistemi di posta elettronica non garantiscono le misure di sicurezza previste per legge e

quelle stabilite dalla stessa per assicurare la riservatezza delle informazioni trasmesse. Pertanto, per garantire la riservatezza delle informazioni trasmesse, si richiede agli utenti di valutare con attenzione l'invio di informazioni contenenti dati personali e/o critici per la CSEA e di adottare gli accorgimenti corrispondenti (es. cifratura preferenzialmente asimmetrica del file, zip con password, etc.) a protezione di tali informazioni;

- è strettamente proibito inviare credenziali o password via e-mail o chat. Le password dovranno essere comunicate esclusivamente a voce o tramite SMS;
- limitare l'invio di messaggi con allegati di grandi dimensioni anche nel rispetto delle soglie imposte. Per tali finalità, si richiede di utilizzare strumenti di compressione dati per ridurre la dimensione dei file allegati di grosse dimensioni;
- adottare comportamenti volti al contenimento dell'occupazione dello spazio mail-box assegnato: per esempio, cancellare o archiviare periodicamente i messaggi presenti sul mail server ed eliminare i messaggi di scarsa importanza di cui non si ravvede la necessità di conservazione;
- si raccomanda, inoltre, di limitare le persone destinatarie delle e-mail esclusivamente a quanto strettamente necessario. Il proliferare, infatti, dell'e-mail dovuto alla cattiva abitudine di inserire in CC o tra i destinatari ulteriori soggetti costituisce un aggravio non necessario delle attività lavorative altrui.

È fatto espresso divieto di:

- utilizzare le caselle di posta elettronica aziendale per motivi non attinenti allo svolgimento delle mansioni (es.: per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, invio e ricezione foto), salvo diversa ed esplicita autorizzazione scritta;
- inviare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi;
- inviare catene telematiche (o "di Sant'Antonio"). Nel caso in cui si dovessero ricevere messaggi di tale tipo, l'utente dovrà comunicarlo immediatamente all'Amministratore di Sistema. Non si deve, in alcun caso, aprire/cliccare su/attivare gli allegati di tali messaggi;
- installare versioni del client diverse da quella fornita o utilizzare altri client di posta elettronica se non espressamente autorizzati da ASI;
- inviare allegati di cui non si sia verificata la provenienza nonché la sicurezza informatica tramite scansione con antivirus;
- utilizzare caselle di posta personali via web (es.: Gmail, Libero, Alice, Tiscali, ecc.), salvo diversa ed esplicita autorizzazione del Responsabile dietro comprovata motivazione di esercizio delle attività lavorative;
- inviare comunicazioni di posta elettronica impiegando l'identità (account di posta elettronica e/o nominativo) di un'altra persona, salvo specifica autorizzazione (delega da parte del proprietario dell'account da utilizzare).

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati pesanti non necessari.

Si richiede che ciascun utente, sul proprio *client* di posta elettronica della CSEA, configuri l'inserimento automatico, su ogni e-mail inviata, del testo standard aziendale che specifica le clausole di riservatezza e i comportamenti da seguire nei casi di invio per errore.

Nei soli casi in cui sia consentito l'acceso web a caselle di posta personali private, i dipendenti sono, comunque, tenuti ad evitare il download di allegati che possano essere veicolo di virus o di elementi dannosi per l'integrità del sistema informativo.

È obbligatorio utilizzare con prudenza tutti gli allegati (*file attachments*) di posta elettronica e verificare che gli stessi non presentino virus e/o altri codici malevoli.

Le "*unsolicited emails*" (c.d. "SPAM") vanno cancellate immediatamente, senza leggerne il contenuto né aprirne gli eventuali allegati.

Nel caso in cui, a seguito di assenza improvvisa o prolungata di un dipendente e per improrogabili esigenze legate all'attività lavorativa, la CSEA ravvisasse la necessità di accedere alle comunicazioni pervenute all'indirizzo di posta elettronica del lavoratore assente, quest'ultimo potrà delegare un altro utente alla verifica del contenuto dei messaggi e all'inoltro al Responsabile di quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Il lavoratore potrà, successivamente, aggiornare/modificare la delega conferita, anche per ragioni organizzative e/o interne dovute a cambiamenti di ruolo e/o nei rapporti di lavoro.

Ove l'utente non conferisca tale delega, la CSEA si riserva la possibilità di procedere mediante personale appositamente autorizzato (ad esempio, l'Amministratore di Sistema) all'attivazione delle specifiche funzionalità di sistema che permetteranno la risposta automatica (auto-reply) ai messaggi e-mail. Di tale circostanza sarà dato avviso tramite e-mail al Responsabile.

I messaggi ricevuti in ogni caso non saranno recapitati altro lavoratore.

Inoltre, al fine di garantire il normale svolgimento dell'attività lavorativa e di assicurare la riservatezza della corrispondenza, nonché in conformità con le indicazioni del Garante, l'utente deve avvalersi delle funzionalità messe a disposizione dal sistema di posta elettronica, che consentono, in caso di assenze programmate (per esempio per ferie o attività di lavoro fuori sede), l'invio automatico di messaggi di risposta contenenti i riferimenti di indirizzi di posta elettronica e telefonici di un altro soggetto incaricato a sostituirlo, o altre modalità di contatto dell'unità di appartenenza.

È vietato, in ogni caso:

a) eseguire il download di files eseguibili o di documenti/files, in qualsiasi formato essi siano, per finalità estranee al rapporto di lavoro o se provenienti da siti internet non conosciuti;

b) leggere messaggi di posta elettronica di provenienza incerta e/o che contengono allegati non ben identificati e/o che presentino un oggetto particolare (es. “I Love you!”, “Consegna corriere.” o formulazioni in un italiano non corretto o non adeguate alla comunicazione).

Cancellazione delle e-mail

La disattivazione/sospensione di un account di posta elettronica è un processo che viene avviato solo nei seguenti casi:

a) cessazione del rapporto di lavoro;
b) scadenza della validità dell’account (es. nel caso di guest/soggetti esterni-/contratti a scadenza), se prevista;
c) superamento dei tentativi di autenticazione errati, di cui alle policy dell’Ente inerenti al controllo accessi;
d) non utilizzo dell’account per un periodo di tempo superiore a quello preventivamente definito nelle policy dell’Ente inerenti al controllo accessi;
e) rilevazione della compromissione, o sospetta compromissione, attraverso la segnalazione da parte dell’utente associato o da incidenti di sicurezza (es. accesso non autorizzato ai sistemi effettuato con l’utenza di cui sopra).

In caso di cessazione del rapporto di lavoro, la CSEA informa il dipendente che l’account sarà immediatamente "disattivato", compatibilmente con i tempi tecnici di predisposizione delle misure atte a finalizzare tale attività; inoltre, la CSEA procede all’attivazione di un "messaggio di mancato recapito" in caso di tentato invio di una comunicazione elettronica sull’account. La disattivazione viene realizzata secondo modalità tali da inibire in via definitiva la ricezione in entrata di ulteriori messaggi diretti al predetto account, nonché la conservazione degli stessi su server aziendali.

L’adozione di tali misure tecnologiche ed organizzative consente di contemperare l’interesse della CSEA ad accedere alle informazioni necessarie all’efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi.

Successivamente alla cessazione del rapporto di lavoro, in assenza di particolari esigenze tecniche o di sicurezza, la CSEA può:

a) conservare temporaneamente le e-mail, in ingresso e in uscita, dell’account di posta elettronica aziendale relative al periodo nel quale il rapporto di lavoro era in essere per la sola finalità specifica e comprovata del trattamento;
b) effettuare la conservazione anche in relazione: (i) ad esigenze tecniche ed organizzative o di sicurezza del tutto particolari; (ii) all’indispensabilità del dato rispetto all’esercizio o alla difesa di un diritto in sede giudiziaria; (iii) all’obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell’autorità giudiziaria o della polizia giudiziaria.

I periodi di conservazione saranno proporzionati alle finalità del trattamento e conformi alla normativa in materia di protezione dei dati personali, con particolare riferimento ai principi di minimizzazione e di limitazione della conservazione dei dati ai sensi dell’art. 5, par. 1, rispettivamente lett. c) ed e), del GDPR.

Se necessario e ove ne ricorrano i presupposti, la CSEA effettuerà una Valutazione d'impatto ex art. 35 del GDPR.

A seguito dello scadere dei già menzionati termini di conservazione, le e-mail saranno cancellate.

La CSEA, per esigenze di sicurezza e di corretto funzionamento dei propri sistemi informatici e telematici, può raccogliere alcune informazioni inerenti all'uso della posta elettronica (es. traffico e-mail in entrata e in uscita che include i log di transazione dei messaggi, i messaggi di posta, gli allegati e i dati esteriori dei messaggi).

Per utenze considerate "critiche" (es. vertici aziendali), inoltre, possono essere installati sistemi di controllo che consentano la raccolta e conservazione delle informazioni relative ad operazioni effettuate sulle suddette caselle e alla modifica dei privilegi di accesso alle stesse assegnati. Tali informazioni potranno essere utilizzate anche a fini di controllo sulla base di quanto stabilito nel presente Regolamento.

Liste di distribuzione

Per facilitare l'interscambio di informazioni relative a finalità istituzionali, è previsto l'uso delle liste di distribuzione (mailing list), personali o centralizzate. L'utente può avvalersi di liste di distribuzione personali, per le proprie necessità funzionali, a fronte di esigenze tecniche e/o gestionali. Una lista generale di distribuzione, centralizzata e comprendente tutti gli utenti, è gestita dall'Amministratore di Sistema.

Oltre alla lista generale di distribuzione, sono possibili altre liste centralizzate (o gruppi) utili a soddisfare le esigenze di categorie omogenee di utenti; l'attivazione di questi gruppi è a cura dell'Amministratore di Sistema che valuterà, di volta in volta, le specifiche richieste.
Si fa presente che l'utilizzo di tali liste permette l'accesso ai messaggi da parte di tutti gli iscritti alla lista di distribuzione collegata a quell'indirizzo. Per tale motivo, sugli account di tali liste non può essere garantita la riservatezza delle comunicazioni.
Le informazioni aziendali riservate, inoltre, sono segrete e oggetto di specifica tutela e, come tali, sono sottoposte a misure di sicurezza adeguate.

A tal fine, pertanto, si specifica che:

- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, handicap o stato di salute o che costituiscano comunque condotta illecita;
- è vietato l'inoltro dei messaggi ricevuti sull'account di posta aziendale ad altro indirizzo e-mail personale dei dipendenti;
- è severamente vietato inviare messaggi, in cui siano presenti allegati file con contenuti inerenti alle attività lavorative, a destinatari che non siano in relazione con le suddette attività e/o non siano autorizzati a riceverli, salvo espressa autorizzazione di ASI.

Utilizzo della rete aziendale

- Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file, che non sia legato all'attività lavorativa, non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup da parte della CSEA.
- Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure descritte nel presente Regolamento. È assolutamente vietato accedere alla rete ed ai programmi autenticandosi con credenziali altrui.
- Qualora si venga in possesso, o si posseggano già, credenziali di rete (o, comunque, di ogni altro sistema) che non siano state assegnate esclusivamente e nominalmente all'utente, questi è tenuto a darne pronta notifica ad ASI.
- L'Ente può, in qualunque momento, procedere alla rimozione di ogni file o applicazione che si ritenga essere un pericolo per la sicurezza su tutti gli asset informatici assegnati e sulle unità di rete.
- Costituisce buona regola il periodico riordino e pulizia degli archivi (almeno ogni tre mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante che, oltre ad occupare le risorse di spazio, costituisca anche fonte di confusione, fermi gli opportuni backup.
- Le cartelle ad accesso condiviso della rete aziendale sono sottoposte a controlli da parte di personale ASI, per monitorare eventuali permessi non appropriati di lettura/scrittura, che potrebbero ampliare il rischio di cancellazioni erronee o modifiche inopportune ai files. Con riferimento alle stampanti collegate alla rete aziendale è cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi dei dispostivi di stampa e copia comuni. È buona regola evitare di stampare documenti o file non adatti (perché, ad esempio, molto "pesanti") su stampanti comuni. Si ricorda che, in caso di necessità, la stampa in corso può essere cancellata.
- Non è consentito effettuare transazioni (finanziarie, di remote banking, acquisti on-line, prenotazioni, ecc.) tramite la rete aziendale.

Qualunque dispositivo, prima di essere connesso alla rete aziendale, deve, in ogni caso, essere sottoposto al controllo di ASI.

Uso della rete Internet e dei relativi servizi

La connessione ad Internet è resa disponibile da parte della CSEA ai fini dello svolgimento dell'attività lavorativa. È, tuttavia, tollerata, in via eccezionale, la navigazione Internet per finalità non direttamente correlate alla prestazione lavorativa, purché ciò avvenga per una durata limitata e tale da non incidere sulla propria prestazione lavorativa e, comunque, in modo da non mettere a repentaglio la disponibilità, l'integrità e la riservatezza dei dati e del sistema informatico della CSEA, ovvero, provocare per lo stesso un danno di immagine.

Ciò comporta che, fermo restando il rispetto delle disposizioni di legge in materia, dell'etica della CSEA, degli obblighi di riservatezza e degli standard previsti da specifiche disposizioni interne, l'utente non può utilizzare

l'accesso ad Internet per motivi personali, se non in maniera breve ed occasionale e, comunque, con modalità che non arrechino intralcio/rallentamento alla normale attività lavorativa propria e di terzi.

È fatto divieto all'utente il downloading di files di varia natura e/o di software – anche se freeware e/o shareware - da siti web e/o da piattaforme peer to peer, distribuite o simili (quali ad esempio BitTorrent, nodi di blockchain, ecc.). Parimenti, non è permesso l'utilizzo di programmi P2P di telefonia o l'uso di programmi di "Instant messaging" non autorizzati da ASI, neanche tramite pagine web. L'unico programma di Instant Messaging autorizzato è Microsoft Teams.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat (esclusi i già citati strumenti autorizzati) e di mailing-list e newsletter non attinenti all'attività lavorativa.

Il lavoratore è tenuto ad utilizzare, esclusivamente, connessioni private, siano esse fornite dalla CSEA o disponibili presso altro luogo privato in cui il lavoratore svolge l'attività lavorativa, come previsto dall'Accordo Quadro di Smart Working. Rimane, in ogni caso, escluso l'utilizzo di connettività pubblica (offerta ad esempio da bar, ristoranti, centri commerciali *et similia*) poiché foriera di potenziali rischi informatici.

Non è consentito l'utilizzo di social network, la partecipazione a forum e gruppi di discussione, l'utilizzo di sistemi di chat, di bacheche elettroniche e/o la registrazione a newsletter, anche utilizzando pseudonimi, salvo diversa ed esplicita autorizzazione del proprio Responsabile, laddove tale attività sia parte integrante delle mansioni assegnate.

La pubblicazione di materiale inerente alla CSEA (es. comunicati stampa, brochure, note interne, ecc.) sui social network può essere effettuata solo previa autorizzazione da parte del proprio Responsabile.

È vietato esprimersi in nome e per conto della CSEA senza preventiva autorizzazione. In assenza di autorizzazione, nel rispetto delle altre regole previste dal presente Regolamento, l'utente deve indicare che il contenuto della comunicazione espressa rappresenti esclusivamente la propria posizione personale. È, altresì, vietato esprimere opinioni su Internet utilizzando il nome ed i dati della CSEA e il dominio ad essa associato, ovvero account riconducibili direttamente o indirettamente all'Ente, se non espressamente autorizzati.

Per esigenze di sicurezza legate alla navigazione in internet e ad una migliore gestione del servizio rispetto agli usi lavorativi, l'utilizzo dei sistemi informativi dell'Ente per la navigazione in internet potrà essere monitorato dalla CSEA attraverso soluzioni software che raccolgono informazioni relative all'utente, che ha condotto la navigazione (es. indirizzo IP), alla URL visitata, data e ora, e ad eventuali eventi di sicurezza relativi alla navigazione stessa (violazione di eventuali policy di content filtering e/o site blocking). Si precisa che il monitoraggio non riguarda il contenuto delle pagine web visualizzate. Tali informazioni possono essere utilizzate anche a fini di controllo sulla base di quanto stabilito nel presente Regolamento.

Uso del software antivirus ed antimalware

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della CSEA mediante virus o mediante ogni altro software, che possa arrecare danno al sistema o ai dati in esso gestiti.

Il sistema informatico presenta software di protezione che vengono aggiornati automaticamente. Si raccomanda, pertanto, di verificare periodicamente l'effettivo funzionamento del sistema e di non disattivare tali software.

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

- sospendere ogni elaborazione in corso, spegnendo il computer il più rapidamente possibile in maniera forzosa (tenendo premuto il tasto "OFF");
- segnalare tempestivamente l'accaduto ad ASI.

Non è consentito l'utilizzo di supporti (chiavi USB, HD Drive, cd rom, DVD, schede di memoria, etc.) di provenienza ignota.

Ogni dispositivo ottico o magnetico (il cui uso sia stato preventivamente autorizzato) deve essere verificato mediante il programma antivirus in dotazione prima del suo utilizzo e, nel caso venga rilevato un virus o malware, il problema deve essere segnalato tempestivamente ad ASI.

Buone prassi di sicurezza informatica

Oltre a quanto già esposto nel presente documento, si riportano alcune indicazioni essenziali per una corretta prevenzione da attacchi (c.d. "igiene informatica"):

- cambiare periodicamente (ogni 30 gg circa) la password e non salvarla nei browser. È possibile cambiare la password a questo link: https://passwordreset.microsoftonline.com/.
- Laddove tecnicamente possibile, utilizzare sempre password differenti per gli applicativi della CSEA (es. una password per Gestione Progetti diversa dalla password delle e-mail).
- Non utilizzare MAI le password utilizzate per gli applicativi della CSEA in altri ambiti.
- Collegarsi sempre con la VPN della CSEA mentre si lavora. Non installare né usare mai ulteriori VPN, né sistemi di *Onion Routing* (es. Tor).
- Non usare sistemi operativi diversi da quello fornito dalla CSEA, neanche in modalità *live*.
- Non accedere mai al deep web/dark web.

Segnalazione di eventuali criticità nell'utilizzo di dati e sistemi

Il furto, lo smarrimento, il danneggiamento, il malfunzionamento, la manomissione dei sistemi assegnati o la violazione dei sistemi di sicurezza devono essere prontamente segnalati ad ASI, fermo restando il rispetto di quanto previsto dalla "*Procedura per la gestione e la notifica del data* breach" vigente.

In caso di furto, occorre allegare alla suddetta segnalazione copia della denuncia effettuata, specificando la tipologia di dati presenti sul dispositivo, nonché eventuali accessi diretti ai sistemi/servizi della CSEA.

Deve essere riferita, tempestivamente, al Responsabile di riferimento la rilevazione o la determinazione, anche involontaria, di ogni episodio che ponga la CSEA nella condizione di violare leggi a tutela del diritto d'autore e della proprietà intellettuale, incluse le norme in materia di tutela dei programmi per

elaboratore (es. software), nonché le norme in materia di protezione dei dati personali e le norme in materia di reati informatici.

Monitoraggio delle attività

Al fine esclusivo di difendere il suo patrimonio informativo, la CSEA adotta misure tecniche idonee a prevenire e rilevare usi illeciti o abusi dei servizi informatici.

A questo scopo la CSEA predispone la registrazione delle attività degli utenti (file di Log) in modalità conforme alle disposizioni di legge e salvaguardandone i diritti.

Trattamento dei file di Log

I file di log sono utilizzati per le seguenti finalità:

- garantire la sicurezza informatica, allo scopo di ricercare ed individuare eventuali agenti automatici malevoli, presenti sulla rete interna della CSEA o per prevenire potenziali minacce informatiche (DDoS, brute force, siti di phishing, truffe informatiche ai danni del dipendente o della CSEA, ecc.);
- risalire all'autore di accessi Internet o di e-mail inviate per esclusive finalità legate alla repressione di reati e su richiesta da parte dell'Autorità Giudiziaria;
- consentire la risoluzione di problemi tecnici legati all'utilizzo degli strumenti informatici della CSEA;
- consentire di identificazione di eventuali comportamenti non consentiti;
- effettuare il monitoraggio prestazionale e funzionale dei servizi informatici a disposizione degli utenti;
- condurre analisi statistiche, in forma aggregata ed anonima, senza associazione esplicita fra l'utente e i dati di traffico.

Con particolare riferimento ai log di navigazione Internet, l'analisi dei log per l'identificazione di eventuali comportamenti non consentiti e l'analisi statistica (per esempio, i siti Web più visitati, i file scaricati, la banda di connessione utilizzata, il numero di pagine visitate, ecc.) vengono condotte attraverso log anonimizzati o aggregati senza associazione esplicita fra l'utente e i dati di traffico, in modo da precludere l'identificazione degli utenti stessi. A fronte dell'accertata esistenza di violazioni, possono essere condotti controlli più circoscritti fino all'individuazione del soggetto autore della violazione.

Il trattamento dei dati di log è consentito esclusivamente a personale espressamente autorizzato. Ai fini del monitoraggio dei servizi, non è, comunque, consentito ad alcuno, ivi inclusi i soggetti sopra citati, di prendere visione del contenuto dei messaggi di posta elettronica, degli allegati e delle pagine Web visitate.

L'Ente, a fronte di anomalie o presunti incidenti di sicurezza, può adottare misure straordinarie per la verifica e la prevenzione di eventuali comportamenti anomali. Tali misure vengono adottate nel rispetto dei principi di pertinenza e non eccedenza. Le attività sono svolte solo da soggetti autorizzati e nel rispetto della normativa sulla protezione dei dati personali e del principio di segretezza della corrispondenza.

Conservazione dei file di Log

In conformità con le direttive del Garante Privacy, la configurazione dei sistemi informatici prevede la cancellazione periodica ed automatica dei file di log (per esempio mediante meccanismi di sovrascrittura

come la rotazione dei file di log) contenenti dati personali relativi agli accessi ad Internet e alla posta elettronica, la cui conservazione non sia necessaria. Allo scadere del periodo di conservazione, i log sono cancellati in via definitiva, fatta salva la possibilità di conservarne aggregati statistici che non possano in alcun modo ricondurre all'identità dell'utente.

In generale, i dati di log sono conservati per il tempo strettamente limitato al perseguimento di finalità organizzative, gestionali e di sicurezza.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Controlli e sanzioni

L'Ente si riserva di effettuare, nel rispetto della normativa vigente, i controlli ritenuti opportuni o necessari inerenti ai sistemi informativi, alle strumentazioni informatiche aziendali, a internet e alla posta elettronica e, in generale, al rispetto delle norme e disposizioni dell'Ente al fine di:

- preservare il proprio patrimonio informativo e tecnologico, anche sotto il profilo della sicurezza;
- salvaguardare i documenti di lavoro;
- garantire la continuità dell'attività lavorativa;
- ricercare e raccogliere elementi di prova inerenti ad un illecito civile, penale, contrattuale o extracontrattuale, o comunque a comportamenti contrari alle disposizioni vigenti e/o comunque in contrasto con le previsioni interne dell'Ente;
- dare riscontro ad una richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

Tali controlli saranno:

- "aggregati" per gruppi ampi di dipendenti e non nominativi, qualora siano mirati esclusivamente a verificare, in linea generale, il corretto utilizzo delle strumentazioni dell'Ente;
- "occasionali" e, in particolare, nel caso in cui emergano indizi generici e non ascrivibili a specifici dipendenti di irregolare utilizzo delle dotazioni aziendali o di inosservanza delle norme e disposizioni della CSEA;
- "mirati", sulla base di elementi o indizi di prova inerenti alla commissione di un illecito civile, penale, contrattuale o extracontrattuale, ovvero inerenti a comportamenti di uno specifico dipendente contrari alle disposizioni vigenti e/o comunque in contrasto con le previsioni interne dell'Ente.

Con riferimento ai controlli “occasionali”, si dà avviso al dipendente e al Responsabile di riferimento tramite e-mail con congruo preavviso, ove ritenuto opportuno. Qualora, tuttavia, si riscontrassero abusi reiterati, i controlli “occasionali” potranno essere effettuati senza preavviso.

Con riferimento ai controlli mirati, prima della effettuazione degli stessi, non verrà dato avviso preventivo.

È fatto, quindi, obbligo a tutti i lavoratori di osservare le disposizioni portate a conoscenza con il presente Regolamento. La CSEA si riserva il diritto di intraprendere azioni disciplinari nei confronti dei dipendenti che contravvengano alle disposizioni di cui al presente Regolamento e/o per fatti disciplinarmente rilevanti che dovessero emergere all’esito dei controlli.

La CSEA si riserva, in ogni caso, la facoltà di intraprendere ogni azione legale che si rendesse necessaria in conseguenza dell’uso improprio o illecito dei beni e degli strumenti dell’Ente nonché di avvisare l'autorità giudiziaria preposta.

Aggiornamento e revisione del Regolamento

Il presente Regolamento troverà applicazione a far data dal giorno successivo all’approvazione da parte del Comitato di gestione ed è soggetto a revisione periodica, in particolare, sulla base di specifiche previsioni normative o esigenze dell’Ente e sostituisce ogni altro atto o documento o comunicazione precedentemente adottati in materia.

Roma, lì 29 agosto 2022

Per presa visione, _____