CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE

DISCIPLINARE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA RETE INFORMATICA E TELEMATICA (INTERNET E POSTA ELETTRONICA) E DEL SISTEMA DI TELEFONIA

Approvato dal Consiglio di Amministrazione in data 22 luglio 2026

Indice

Premessa

Il Garante per la privacy, con la Deliberazione, n. 13 del 1° marzo 2007, nell'emanare le linee guida in tema di corretto utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro, ha precisato al punto 3.2 che "può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (...) e da sottoporre ad aggiornamento periodico".

Tenuto conto della normativa di settore, in particolare anche di quanto disposto dal Decreto Legislativo n. 196/2003 recante il "Codice in materia di protezione dei dati personali", come modificato dal D. Lgs. n. 101/2018, recante le "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio (il "**GDPR**"), si reputa necessario promuovere:

- ✓ in modo chiaro e particolareggiato le modalità per il corretto utilizzo degli strumenti informatici messi a disposizione e se, in quale misura e con quali modalità, possano essere effettuati eventuali controlli;
- ✓ l'adozione di misure organizzative e tecnologiche volte a prevenire utilizzi impropri degli strumenti informatici, minimizzando in ogni evenienza l'uso dei dati riferibili ai dipendenti e comunque nel rispetto dei principi di necessità, pertinenza e non eccedenza;
- ✓ la corretta applicazione delle disposizioni del Garante della Privacy relative all'utilizzo degli strumenti elettronici ed al possibile controllo dell'operato dei dipendenti, in equilibrato bilanciamento delle esigenze di tutela dei beni rilevanti del MOST e dei diritti alla riservatezza e dignità dei soggetti coinvolti.

A tal fine, il presente Disciplinare per il corretto utilizzo degli strumenti informatici, della rete informatica e telematica (internet e posta elettronica) e del sistema di telefonia (il "**Disciplinare**") sintetizza le regole per l'utilizzo delle risorse informatiche nell'ambito delle strutture del Centro Nazionale per la Mobilità Sostenibile (il "**MOST**").

Ai fini del presente Disciplinare, per "**Utente**" si intende il soggetto assegnatario degli strumenti informatici. Ai fini privacy, l'utente agisce anche in veste di "Soggetto Autorizzato" al trattamento dei dati personali ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, operando secondo le specifiche istruzioni fornite dal MOST.

Sezione I - DISPOSIZIONI GENERALI

Articolo 1 – Finalità

1. Le disposizioni contenute nel presente Disciplinare hanno lo scopo principale di adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici messi a disposizione da MOST per lo svolgimento delle mansioni attribuite, delle reti e della posta elettronica e per definire il diritto di MOST di effettuare verifiche mirate e graduali sul corretto uso dei suddetti strumenti, esclusivamente per comprovate esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto dello Statuto dei Lavoratori (Art. 4, L. n. 300/1970) e della normativa in materia di protezione dei dati personali.
2. MOST, quale datore di lavoro, assegna le risorse informatiche qualificandole come strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, ai sensi dell'art. 4, secondo comma, dello Statuto dei Lavoratori. In conformità alla disciplina in materia di privacy, MOST adotta misure tecniche e organizzative idonee ad escludere qualsiasi forma di monitoraggio massivo, prolungato e indiscriminato sull'attività dei dipendenti, limitando gli eventuali accertamenti a interventi mirati, proporzionati e necessari alla salvaguardia della sicurezza delle reti e del patrimonio aziendale.
3. In particolare, il presente Disciplinare è diretto a:
   a) porre in essere ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri degli strumenti informatici, della rete informatica e telematica e del sistema di telefonia, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza;
   b) informare coloro che utilizzano per lavoro gli strumenti informatici, la rete informatica e telematica e il sistema di telefonia messi a disposizione dal MOST delle misure adottate e che si intendono adottare al fine di:
      - ✓ garantire il diritto alla riservatezza degli utenti interni ed esterni della rete informatica, telematica e di telefonia;
      - ✓ assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;

- ✓ prevenire rischi alla sicurezza del sistema;
- ✓ responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- ✓ definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

Articolo 2 – Principi generali

1. MOST promuove il corretto utilizzo degli strumenti informatici, della rete informatica e telematica, con particolare riferimento all'uso di internet, alla posta elettronica e del sistema di telefonia quali strumenti utili a perseguire le proprie finalità istituzionali, nel rispetto dei principi e delle linee guida delineati dalla normativa vigente.
2. La titolarità dei beni e degli strumenti informatici, telematici e di telefonia è in capo a MOST. Tali strumenti sono messi a disposizione del personale dipendente e tale dotazione non costituisce titolo per l'acquisizione di alcun diritto in capo ai predetti soggetti e può essere ridotta, sospesa o eliminata qualora ne sussistano le motivazioni.
3. Ogni dipendente, dopo aver ricevuto le relative istruzioni, è responsabile, sotto i profili civili e penali, del corretto uso degli strumenti informatici, telematici e di telefonia e del contenuto delle comunicazioni effettuate. Risponde dei danni, anche all'immagine di MOST, che possono derivare da comportamenti illeciti.
4. MOST privilegia l'attività di prevenzione rispetto a quella di controllo, indicando ed attuando, in un'ottica di reciproco affidamento, appropriate misure di tutela e promuovendo misure di autotutela da parte dei fruitori, nonché assicurando la massima diffusione al contenuto del presente Disciplinare.
5. Nello svolgimento dell'attività di monitoraggio e controllo, MOST agisce nel rispetto della normativa vigente, con particolare riguardo alla tutela dei diritti dei lavoratori e alle garanzie in materia di protezione dei dati personali, nell'osservanza dei principi di ragionevolezza, correttezza, trasparenza e proporzionalità.

Articolo 3 – Destinatari

1. Le disposizioni contenute nel presente Disciplinare si applicano a tutti i lavoratori dipendenti del MOST e a tutto il materiale di proprietà o noleggiato da MOST.
2. Le prescrizioni del presente Disciplinare integrano le specifiche istruzioni impartite agli autorizzati in materia di trattamento dei dati personali ai sensi del GDPR.
3. Il mancato rispetto delle regole e dei divieti di cui al presente Disciplinare costituisce, per i dipendenti, una condotta illecita del lavoratore che può comportare, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo di Lavoro vigente, fatto salvo comunque il diritto di MOST al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore.
4. Per quanto riguarda i collaboratori esterni e gli addetti in outsourcing, si applicano le disposizioni di cui all'articolo 12 del presente Disciplinare.

Sezione II - USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Articolo 4 – Criteri generali di utilizzo

1. Gli strumenti informatici (a titolo esemplificativo personal computer, stampanti, ecc.), telematici (a titolo esemplificativo accesso ad internet, tramite collegamento fisso o mobile, la posta elettronica), telefonici (a titolo esemplificativo telefono fisso), messi a disposizione da MOST, costituiscono strumento di lavoro.
2. Pertanto, l'utilizzo di essi è consentito, di regola, per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative, comprese quelle interne, nonché delle esigenze di funzionalità e di sicurezza dei sistemi informativi.
3. Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali ad esempio quelle che attengono allo svolgimento del rapporto di lavoro.
4. Il personale deve custodire e utilizzare gli strumenti affidatigli in modo appropriato, con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza del sistema. Gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel presente Disciplinare e tale configurazione non deve essere modificata senza la

preventiva necessaria autorizzazione degli Amministratori di Sistema o di chi ne abbia la competenza. Il personale è altresì tenuto ad informare direttamente il proprio responsabile nell'ipotesi di furto, danneggiamento o malfunzionamento, anche parziale, degli strumenti e/o del sistema.

5. Gli utenti che non dispongono di uno smartphone aziendale e utilizzano un dispositivo personale per il secondo fattore di autenticazione (2FA) tramite app di autenticazione (es. Microsoft Authenticator) sono tenuti a garantire la sicurezza del proprio device. In caso di smarrimento, furto o compromissione del dispositivo personale utilizzato per l'autenticazione, l'autorizzato è obbligato a informare tempestivamente gli Amministratori di Sistema al fine di disabilitare il secondo fattore associato e attivare le necessarie misure di sicurezza per la protezione dell'account e delle risorse aziendali. Il mancato tempestivo avviso potrebbe esporre l'organizzazione a rischi di sicurezza e sarà considerato una violazione delle policy aziendali in materia di sicurezza informatica.

Articolo 5 – Utilizzo degli strumenti informatici

1. L'accesso alla stazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password/PIN). Per l'uso, la scelta, la modifica e la custodia delle credenziali si rinvia a quanto stabilito dalle regole di Microsoft consultabili al seguente link https://learn.microsoft.com/it-it/entra/identity/authentication/concept-sspr-policy#microsoft-entra-password-policies.
2. È vietato:
   a) installare sulla stazione di lavoro software, anche se gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati da MOST e collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'organizzazione;
   b) alterare, disattivare o modificare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica e di ogni altro software installato sulle attrezzature e sugli strumenti, fissi e mobili (postazione di lavoro, notebook, tablet, cellulari, altri supporti, ecc.), forniti in dotazione al personale. Inoltre, l'autorizzato/l'utente ha il dovere di usare e gestire le attrezzature e gli strumenti ricevuti in dotazione con attenzione e diligenza, nonché quello di segnalare

tempestivamente all'amministratore di sistema e/o al responsabile ogni anomalia o disfunzione al fine di ripristinare il corretto funzionamento degli stessi;

c) accedere al Bios delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate;

d) caricare o detenere nelle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, quando questi comportamenti interferiscano con le mansioni attribuite, ovvero aggravino i rischi connessi all'utilizzo dei relativi strumenti;

e) in ogni caso, caricare, detenere e/o stampare materiale informatico:

- il cui contenuto (a mero titolo esemplificativo: testo, audio, video) sia chiaramente tutelato dal diritto d'autore. Nel caso in cui ciò sia necessario per la propria attività lavorativa, l'autorizzato è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
- il cui contenuto sia contrario a norme di legge.

4. Le modifiche alla configurazione delle stazioni di lavoro possono essere effettuate unicamente da soggetti espressamente e formalmente autorizzati da MOST. Il personale non è autorizzato a modificare il sistema, neppure se si tratta della postazione di lavoro assegnata.
5. A titolo esemplificativo, ma non esaustivo, sono considerate modifiche del sistema:
   a) modificare i collegamenti di rete esistenti;
   b) usare dispositivi removibili (CD, dvd, hard disk, floppy, ecc.) per alterare la procedura di avvio del dispositivo ed in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito da MOST;
   c) aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;
   d) installare, senza l'assistenza di personale autorizzato, un qualsiasi software, inclusi quelli scaricati da Internet, o comunque alterare la configurazione della stazione di lavoro assegnata.
5. Le cartelle—presenti nei server di MOST 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 questa unità. Su tale unità vengono svolte regolari attività di amministrazione e back up da parte del personale incaricato (Amministratori di Sistema).

Eventuali attività di verifica sui server sono effettuate esclusivamente per finalità tecniche, di manutenzione, di ripristino o per garantire la sicurezza delle reti e delle informazioni dai cyber-attacchi, escludendo qualsiasi finalità di monitoraggio o controllo a distanza dell'attività lavorativa del singolo utente.

6. Al fine di preservare l'integrità e la sicurezza della rete, i sistemi automatizzati di sicurezza (es. antivirus) o il personale tecnico incaricato (Amministratori di Sistema) possono procedere alla rimozione o al blocco di file o applicazioni ritenuti pericolosi. Tali interventi avvengono esclusivamente per comprovate esigenze di sicurezza informatica, escludendo l'accesso sistematico ai contenuti personali o alla corrispondenza del lavoratore.
7. Per problematiche di natura informatica, gli utenti sono tenuti a rivolgersi in prima istanza all'Ufficio ICT. Qualora necessario, l'Ufficio ICT provvederà ad attivare il supporto dei partner tecnologici di riferimento. Tali soggetti terzi operano nel rigoroso rispetto delle istruzioni impartite da MOST.
8. Per l'entrata in organico di nuove risorse è previsto un processo strutturato di on-boarding, disciplinato da apposito vademecum. Le conseguenti attività e le responsabilità sono dettagliate per competenza nel medesimo Vademecum di on-boarding.
9. In caso di cessazione del rapporto di lavoro, è previsto un processo di off-boarding finalizzato alla disattivazione tempestiva degli accessi logici e alla restituzione delle risorse aziendali. In particolare, gli account di posta elettronica nominativi verranno disattivati ed eliminati, previa impostazione di un messaggio di risposta automatica che indichi ai terzi i nuovi riferimenti aziendali da contattare. Non è in alcun caso consentito il reindirizzamento automatico (forward) della posta in arrivo verso altri account aziendali, a tutela della riservatezza delle comunicazioni dell'ex dipendente e dei terzi mittenti.

Articolo 6 – Utilizzo della rete internet

1. L'accesso alla rete Internet costituisce strumento di lavoro ed è consentito, di regola, per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa.
2. È vietato entrare nella rete e nei programmi con un codice di identificazione diverso da quello assegnato. Le credenziali di accesso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni e le procedure impartite.
3. È altresì, vietato:

a) scaricare e/o installare software non espressamente autorizzati da MOST;
b) scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio dell'attività lavorativa, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto;
c) scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia chiaramente tutelato dal diritto di autore;
d) partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non attinenti o connesse all'attività lavorativa;
e) navigare in internet su siti contrari a norme di legge;
f) effettuare ogni genere di transazione finanziaria per fini personali;
g) installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia Peer to Peer (es. eMule, kazaa, bittorrent, ecc.), indipendentemente dal contenuto dei file scambiati.

4. Tutti gli utenti sono tenuti ad adottare un comportamento conforme alle disposizioni del presente Disciplinare e ogni utilizzo improprio potrà essere oggetto di verifica e comportare le conseguenze previste dalla normativa e dai regolamenti interni.

Articolo 7 – Utilizzo dei sistemi di Intelligenza Artificiale

1. MOST può mettere a disposizione del personale, strumenti e applicativi basati su sistemi di Intelligenza Artificiale ("**AI**"), inclusi sistemi di AI generativa integrati negli ambienti di produttività aziendale, esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa e nel rispetto delle disposizioni normative vigenti, delle policy interne e delle istruzioni impartite.
2. È consentito utilizzare tali strumenti di AI autorizzati da MOST anche per il caricamento, l'inserimento o la condivisione di dati, documenti o informazioni aziendali. Il personale è tenuto a rispettare il principio di minimizzazione dei dati, limitando l'inserimento alle sole informazioni strettamente necessarie, adeguate e pertinenti per la finalità specifica. Qualora sia indispensabile elaborare dati personali o informazioni aziendali sensibili, il personale deve preventivamente applicare tecniche di anonimizzazione o pseudonimizzazione per privare i dati del loro potere identificativo diretto e ridurre i rischi di accessi abusivi o violazioni della riservatezza.
3. L'utilizzo dei sistemi di AI deve avvenire nel rispetto dei principi di correttezza, trasparenza, sicurezza, protezione dei dati personali, riservatezza delle informazioni

aziendali. Il personale è responsabile della verifica dell'accuratezza, pertinenza e affidabilità dei contenuti generati dai sistemi di AI prima del loro utilizzo, diffusione o impiego in processi decisionali o operativi.

4. I sistemi di IA costituiscono uno strumento di supporto e non sostituiscono l'autonomia decisionale e la responsabilità del personale. Durante l'impiego di tali sistemi, il lavoratore deve esercitare una costante supervisione umana ed è tenuto a:
   a) mantenere una consapevolezza critica per evitare l'eccessivo affidamento acritico sull'output prodotto dalla macchina (cd. distorsione dell'automazione), conservando sempre la facoltà di ignorare, annullare o ribaltare le raccomandazioni del sistema IA;
   b) verificare scrupolosamente l'accuratezza, la correttezza e l'imparzialità dei risultati, al fine di individuare e correggere eventuali errori, "allucinazioni" o distorsioni (bias);
   c) assicurarsi che l'impiego dei contenuti generati non violi diritti di proprietà intellettuale o il diritto d'autore di soggetti terzi, prestando attenzione ai rischi derivanti dall'addestramento massivo (machine learning) su opere preesistenti.

5. MOST promuove adeguate iniziative di informazione e formazione finalizzate a garantire un utilizzo consapevole e responsabile dei sistemi di AI, in conformità con i principi di alfabetizzazione sull'AI previsti dalla normativa vigente.

Articolo 8 – Utilizzo della posta elettronica

1. MOST mette a disposizione di ogni lavoratore il servizio di posta elettronica, assegnando a ciascun autorizzato caselle di posta istituzionali per fini esclusivamente lavorativi.
2. Al fine di agevolare lo svolgimento dell'attività lavorativa, MOST rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative) affiancandoli a quelli individuali.
3. L'indirizzo di posta elettronica messa a disposizione da MOST, contraddistinto dalla presenza del dominio "@centronazionalemost.it", costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.
4. È escluso, di regola, l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo ripetuto.
5. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di

posta elettronica è scelta e registrata dall'autorizzato nel rispetto dei criteri e delle regole indicati dalle regole di sicurezza definite dalla suite Microsoft.

6. Al fine di un corretto utilizzo della posta elettronica è vietato:
   a) inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno a MOST o a terzi nonché messaggi a catena e/o spam;
   b) scambiare messaggi impersonando un mittente diverso da quello reale;
   c) scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;
   d) aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio.

Articolo 9 – Accesso alla casella di posta elettronica del lavoratore assente

1. Al fine di ottemperare alle vigenti normative, nei casi in cui sia indispensabile ed indifferibile accedere ai dati trattati dai singoli incaricati o agli strumenti informatici in dotazione allo stesso, sia per esigenze aziendali organizzative che per eventuali esigenze di sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), MOST potrà accedere ai dati ed agli strumenti elettronici in uso, mediante intervento degli Amministratori di Sistema debitamente incaricato con procedura tracciata e limitata. A tal proposito, gli addetti alla manutenzione dei sistemi interni ed esterni e gli Amministratori di Sistema saranno autorizzati mediante opportuna lettera di incarico.
2. Il provider di posta elettronica predefinito da MOST consentirà, in caso di assenze programmate, di inviare automaticamente messaggi di risposta.
3. In caso di assenze non programmate o prolungate, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni, MOST disporrà, lecitamente e mediante personale appositamente autorizzato (gli Amministratore di Sistema oppure un loro autorizzato), l'attivazione di un analogo accorgimento di un messaggio di risposta automatica contenente le coordinate di un soggetto alternativo cui trasmettere le

comunicazioni. È in ogni caso escluso il re-indirizzamento automatico (forward) della posta in arrivo verso altre caselle.

4. In caso di assenza del lavoratore prolungata o cessazione del rapporto di lavoro, l'accesso alla casella e-mail istituzionale può essere effettuato solo per comprovate esigenze organizzative, di continuità operativa o tutela del patrimonio informativo di MOST dall'Amministratori di Sistema, con procedura tracciata e motivata. L'accesso è autorizzato dal Direttore Generale e, ove possibile, previa informazione al lavoratore interessato. Tutte le operazioni devono essere documentate e conservate per finalità di accountability. Qualora possibile, il lavoratore è informato in fase di uscita e gli viene richiesto di configurare risposte automatiche o comunicare contatti sostitutivi. In mancanza, sarà attivato un messaggio di risposta automatica con indicazione dell'ufficio di riferimento.
5. Ogni accesso deve essere limitato ai soli messaggi rilevanti per la continuità lavorativa, con esclusione di consultazioni generalizzate. Il principio di minimizzazione deve essere sempre rispettato.
6. In tutti i casi di accesso eccezionale a strumenti informatici o caselle di posta elettronica istituzionali – tra cui, a titolo esemplificativo, quelli relativi a assenze improvvise e prolungate, cessazione del rapporto di lavoro, decesso del lavoratore, indagini interne, o eventi critici per la sicurezza informatica – è sentito il Responsabile della protezione dei dati personali (DPO), al fine di valutare l'adeguatezza dell'accesso rispetto ai principi di necessità, proporzionalità e minimizzazione, nonché per individuare eventuali misure alternative o integrative di tutela.
7. In caso di decesso del lavoratore, eventuali operazioni sulla casella di posta elettronica aziendale potranno essere disposte esclusivamente per esigenze inderogabili di continuità operativa, nel rispetto del principio di minimizzazione e delle disposizioni dell'art. 2-terdecies del D.Lgs. n. 196/2003.
8. L'accesso di cui all'art. 2-terdecies del D.Lgs. n. 196/2003 deve avvenire previa consultazione del Responsabile della protezione dei dati (DPO) e può essere autorizzato dal Direttore Generale, con limite rigoroso ai soli contenuti strettamente professionali, escludendo la consultazione indiscriminata della casella.
9. Nel caso in cui familiari, conviventi o altri aventi causa presentino richiesta di accesso ai contenuti della casella di posta elettronica del defunto, MOST valuterà l'istanza alla luce dei criteri di cui all'art. 2-terdecies del D.Lgs. n. 196/2003, tenendo conto:
    - delle indicazioni eventualmente fornite in vita dall'interessato;

- della prevalenza di un interesse proprio, meritevole di tutela, in ordine alla conservazione della riservatezza;
- della natura strettamente professionale dell'account istituzionale;
- delle finalità per cui è richiesta la disponibilità dei dati.

L'eventuale accoglimento della richiesta sarà subordinato a istruttoria a cura del DPO, anche con eventuale oscuramento selettivo dei contenuti non pertinenti, ove tecnicamente possibile.

Articolo 10 – Utilizzo degli strumenti di telefonia

1. Gli strumenti di telefonia (sia fissa sia mobile) eventualmente messi a disposizione da MOST costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.
2. È escluso, di regola, l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. È in ogni caso vietato l'uso reiterato e prolungato per fini personali. Al fine di garantire il contenimento dei costi, MOST si riserva la facoltà di analizzare l'andamento complessivo del traffico telefonico in base ai dati di fatturazione (su base aggregata o anonimizzata), garantendo in ogni caso la non tracciabilità e la non visibilità delle numerazioni relative alle eventuali comunicazioni effettuate dal lavoratore per esigenze personali.
3. Ciascun autorizzato è responsabile della custodia del dispositivo mobile aziendale a lui assegnato. È fatto obbligo di proteggere l'accesso al dispositivo tramite codici di blocco (PIN, password o biometria) e di non alterare o disattivare le impostazioni di sicurezza prefigurate dagli Amministratori di Sistema.
4. In caso di smarrimento o furto dell'eventuale telefono mobile aziendale, ovvero qualora si sospetti una compromissione dello stesso, il lavoratore è tenuto a darne immediata comunicazione all'Ufficio ICT e al proprio responsabile. La tempestiva segnalazione è condizione indispensabile per consentire a MOST di bloccare le utenze, cancellare i dati da remoto e attivare le necessarie procedure aziendali per la gestione dei Data Breach ai sensi del GDPR.

Sezione III – CONTROLLI

Articolo 11 – Svolgimento dei controlli

1. MOST privilegia misure preventive rispetto ai controlli individuali, ammessi solo nei casi tassativamente previsti dalla legge (esigenze giudiziarie, gravi inadempienze, incolumità di terzi).
2. I controlli sull'uso di web e posta elettronica seguono una logica graduata: prima aggregati e anonimi, poi – solo in caso di persistente anomalia – individuali. Sono vietati controlli sistematici, costanti o indiscriminati.

Sezione IV - DISPOSIZIONI FINALI

Articolo 12 – Utilizzo degli strumenti da parte di collaboratori esterni e addetti in outsourcing

1. L'inquadramento in materia di protezione dei dati personali dei collaboratori esterni e delle società in outsourcing varia in funzione della natura dell'incarico. Tali soggetti operano, a seconda dei casi, in veste di Responsabili del Trattamento (art. 28 GDPR) tramite apposito accordo, o di Titolari Autonomi. Esclusivamente alcune delle persone fisiche che collaborano con MOST rendendo prestazioni di tipo intellettuale ovvero d'opera ai sensi dell'art. 2222 del Codice Civile sono designate quali "soggetti autorizzati" al trattamento ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, operando nel rigoroso rispetto delle istruzioni ricevute.
2. I collaboratori esterni e gli addetti in outsourcing operanti presso le sedi di MOST o da remoto accedono, in base alle mansioni loro attribuite, alla rete internet aziendale e ai servizi interni di rete. Ad alcuni soggetti può inoltre essere assegnato un indirizzo di posta elettronica istituzionale del MOST, previa autorizzazione del Direttore Generale (nome.cognome.ext@centronaziolemost.it)
3. Tali soggetti, salvo diversa previsione contrattuale, utilizzano dispositivi personali (es. notebook, telefono mobile) per lo svolgimento delle attività (approccio BYOD). In ragione di ciò, pur non essendo attive funzionalità di controllo centralizzato o filtraggio automatizzato

su tali dispositivi, gli utilizzatori restano pienamente soggetti agli obblighi di sicurezza e alle limitazioni previsti nel presente Disciplinare.

4. Ai fini della salvaguardia del patrimonio informativo aziendale, i dispositivi personali utilizzati per accedere alla rete o ai dati di MOST devono tassativamente:

   a) disporre di software antivirus/antimalware attivo e regolarmente aggiornato;

   b) essere configurati con credenziali di accesso o sistemi biometrici per impedire accessi non autorizzati e prevedere il blocco automatico dello schermo in caso di inattività.

5. L'accesso alla rete internet e alla intranet da parte di tali soggetti è tracciato nei log di rete del MOST esclusivamente per finalità di sicurezza delle reti e accountability, con tempi di conservazione limitati a quanto strettamente necessario, escludendo ogni monitoraggio indiscriminato.
6. L'uso dell'indirizzo di posta elettronica del MOST da parte di collaboratori esterni è ammesso esclusivamente per finalità lavorative ed è soggetto alle stesse limitazioni previste per il personale interno (Art. 7). In caso di cessazione dell'incarico, la casella e-mail verrà tempestivamente disattivata, con contestuale attivazione di un messaggio di risposta automatica che indichi i nuovi referenti aziendali. La rimozione definitiva dell'account avverrà entro i successivi 30 giorni.
7. Ogni collaboratore esterno e addetto in outsourcing riceve informativa e formazione adeguata sull'uso corretto delle risorse digitali di MOST, in proporzione all'accesso concesso.
8. Le violazioni al presente Disciplinare da parte di soggetti esterni costituiscono inadempimento contrattuale e comportano l'immediata sospensione o revoca dell'accesso alle risorse del MOST, fatto salvo il risarcimento dei danni.
9. L'inizio e la cessazione delle attività oggetto di collaborazione sono disciplinati da un processo strutturato, descritto nei Vademecum di on-boarding e off-boarding, i quali dettagliano le responsabilità di MOST e dei partner tecnologici, in particolare per la tempestiva revoca delle credenziali alla scadenza del contratto.
10. I collaboratori esterni e gli addetti in outsourcing sono tenuti a non inserire dati personali, documenti o informazioni riservate di MOST all'interno di sistemi di Intelligenza Artificiale che non siano stati preventivamente autorizzati da MOST o che non offrano adeguate garanzie di sicurezza e riservatezza.

L'eventuale utilizzo di strumenti basati sull'Intelligenza Artificiale nell'ambito dell'incarico dovrà avvenire nel rispetto delle istruzioni fornite da MOST, delle misure di sicurezza applicabili e degli obblighi di riservatezza assunti contrattualmente. Qualora richiesto, il collaboratore dovrà informare preventivamente MOST dell'impiego di tali strumenti.

Articolo 13 – Informativa

Il contenuto del presente Disciplinare integra l'informativa già fornita ai dipendenti e ai collaboratori ai sensi dell'art. 13 del GDPR, nonché le informazioni dovute ai sensi dell'art. 4, comma 3, della Legge n. 300/1970 (Statuto dei Lavoratori) in merito alle modalità d'uso degli strumenti e all'effettuazione dei controlli.

Articolo 14 – Disposizioni finali

1. Il presente Regolamento entra in vigore dalla data della sua approvazione da parte del Consiglio di Amministrazione della Fondazione.
2. Copia del presente Disciplinare è messa a disposizione di tutti i dipendenti e collaboratori mediante invio a mezzo posta elettronica aziendale e pubblicazione in apposita sezione accessibile all'interno della intranet aziendale.
3. MOST garantisce che il Disciplinare sia sempre consultabile in formato aggiornato e provvede a darne adeguata informativa in occasione di eventuali revisioni, nonché nell'ambito delle attività di formazione e sensibilizzazione del personale.
4. MOST garantisce la revisione periodica del presente Disciplinare e in occasione di aggiornamenti normativi, tecnologici o organizzativi significativi che impattino sulle modalità di utilizzo degli strumenti informatici e telematici.
5. Eventuali modifiche sostanziali saranno tempestivamente comunicate ai destinatari e integrate nei programmi formativi in materia di protezione dei dati personali e sicurezza informatica.