*Ministero della cultura*

MINISTERO DELLA CULTURA

# Disciplinare tecnico
# per l'utilizzo degli strumenti informatici
# e principali misure di sicurezza

(ai sensi del Regolamento UE 679/2016 e dei Provvedimenti del Garante per la protezione dei dati personali)

## *Sommario*

## Riferimenti

[1]. *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) Legge 20 maggio 1970, n. 300;

[2]. *Codice in materia di protezione dei dati personali e relativo disciplinare tecnico*; Decreto legislativo 30 giugno 2003, n. 196;

[3]. *Linee guida del Garante per posta elettronica e internet* emesse dal Garante per la protezione dei dati personali con Deliberazione 13/2007 e pubblicate sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007;

[4]. *Regolamento generale sulla protezione dei dati;* Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

## 1. Introduzione

La *Direzione Generale Organizzazione* (DG-OR) coordina e cura i sistemi informativi centrali e nazionali del MiC, anche attraverso l'emanazione di raccomandazioni, linee guida, standard, raccolta e analisi di buone pratiche, statistiche, studi e rapporti, in attuazione dei principi dell'amministrazione digitale e degli open data e in coerenza con le linee strategiche dell'Agenzia per l'Italia Digitale (AGID).

Il presente documento sostituisce quanto espresso nella Circolare n. 132 del 27 luglio 2016 "*Linee guida per l'utilizzo di risorse informatiche"*.

Il Garante per la privacy, con la Deliberazione 1° marzo 2007, n. 13, 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".*

Il Ministero della cultura ha già pubblicato documenti programmatici[1] con lo scopo di descrivere le modalità di trattamento dei dati effettuato dal Ministero, sotto il profilo della sicurezza e riservatezza, al fine di attestarne la qualità, la puntualità e l'osservanza alle previsioni formulate dal Decreto legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali.*

Tenuto conto della normativa di settore, in particolare anche quanto disposto dal decreto legislativo 10 agosto 2018, n. 101 recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"* 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, tenendo conto altresì della disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali;
- 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 Ministero e dei diritti alla riservatezza e dignità dei soggetti coinvolti.

A tal fine, il presente **Disciplinare tecnico per l'utilizzo degli strumenti informatici e principali misure di sicurezza** sintetizza le regole per l'utilizzo delle risorse informatiche nell'ambito delle strutture centrali e periferiche del Ministero.

[1] Di seguito:
- "*Documento programmatico sulla Sicurezza per il Ministero per i beni e le attività culturali*", emanato in data 31 marzo 2006 con prot. n. 1787;
- "*Documento programmatico sulla Sicurezza in attuazione del decreto legislativo 30 giugno 2003, n.196 recante "Codice in materia di protezione dei dati personali". Notifica e formazio*ne", pubblicato con Circolare 153 del 31 luglio 2006;
- "*Norme operative in materia di sicurezza, emanate in attuazione del decreto legislativo 30 giugno 2003, n.196 recante "Codice in materia di protezione dei dati personali". Notifica e formazione*", pubblicato con Circolare 189 del 12 ottobre 2006;
- "*Documento programmatico sulla Sicurezza – aggiornamento anno 2010*" emanato in data 31 marzo 2010, con prot. n. 13270;
- "*Documento programmatico sulla Sicurezza – aggiornamento anno 2011*" emanato in data 7 marzo 2011, prot. 8207.

## 2. Obiettivi e finalità

L'obiettivo del presente documento è divulgare le politiche che il MiC ha messo in atto per una corretta gestione dei Sistemi informativi a livello centrale e periferico, sia per quanto concerne i documenti conservati su supporto informatico ed i relativi strumenti di gestione che per quelli in formato cartaceo, mediante la formalizzazione di una serie di direttive per tutto il personale coinvolto nel trattamento dei dati. Il presente documento individua quindi, in generale, le misure che devono essere osservate dal personale che, nello svolgimento delle proprie mansioni, gestisce quotidianamente dati personali e sensibili.

Le presenti disposizioni, in attuazione delle *linee guida del Garante per la posta elettronica e internet*[2] , 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 dall'Amministrazione per lo svolgimento delle mansioni attribuite, delle reti e della posta elettronica e per definire con altrettanta chiarezza il diritto dell'Amministrazione a verificare l'uso corretto dei suddetti strumenti ed individuare le modalità con cui l'Amministrazione esercita tale diritto.

Le scelte di base delle presenti disposizioni sono orientate a prevenire usi arbitrari degli strumenti informatici o comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza dei dati, senza ledere, nel contempo, il diritto alla riservatezza degli utenti, a proteggere le libertà fondamentali e la dignità delle persone.

L'Amministrazione, quale datore di lavoro, nella persona del Direttore Generale Organizzazione o di un suo rappresentante (qui di seguito definito Amministrazione) adotta ogni misura volta ad eliminare la possibilità di controllo informatico, nel rispetto dell'art. 4 secondo comma dello Statuto dei lavoratori e della vigente disciplina in materia di privacy.

Il documento, sottoposto ad aggiornamenti periodici per garantire la corrispondenza con la normativa vigente e per implementazioni e modifiche derivanti dall'esperienza, sarà disponibile sul sito Intranet dell'Amministrazione (www.rpv.beniculturali.it).

## 3. Campo di applicazione

Le presenti direttive si applicano a tutti i lavoratori dipendenti del MiC, nonché a tutto il personale che, a qualsiasi titolo presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso le sedi del Ministero e che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato ed abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche del Ministero.

Tale documento si intende applicabile a tutto il materiale di proprietà o noleggiato dal Ministero ed all'utilizzo di eventuali dispositivi privati utilizzati nelle proprie strutture.

Il documento fa riferimento ad usi impropri dell'accesso ad internet e all'uso della posta elettronica solo in relazione a comportamenti che l'Amministrazione ritiene non conformi all'ambito lavorativo.

Per i reati commessi mediante l'uso delle tecnologie informatiche si fa riferimento alla legislazione vigente. L'Amministrazione tuttavia è tenuta ad adottare ogni possibile misura di sicurezza volta a limitare utilizzi indebiti che possano essere fonte di responsabilità per l'utente.

[2] Lavoro: le linee guida del Garante per posta elettronica e internet: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522. Pubblicato nella Gazzetta Ufficiale n° 58 del 10 marzo 2007.

## 4. Direttive generali sul Sistema Informativo e proprietà delle risorse

L'utenza, secondo i parametri definiti nel punto precedente, deve essere consapevole che i dati creati e presenti sui sistemi informatici del Ministero sono di proprietà del medesimo.

A causa della necessità di amministrazione e protezione della rete aziendale, l'utenza deve essere consapevole che l'Amministratore di Sistema, ed in generale, gli operatori addetti alla manutenzione dei Sistemi Informativi, durante le fasi di amministrazione e/o manutenzione della rete o in qualsiasi altro momento, possono accedere volontariamente o incidentalmente a tutti i dati presenti sui sistemi informatici.

Si ricorda che, 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 che per eventuali esigenze di sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), l'ente potrà accedere ai dati ed agli strumenti elettronici mediante intervento delle figure nominate Amministratore di Sistema.

Si precisa inoltre che gli addetti alla manutenzione dei sistemi interni ed esterni e l'Amministratore di Sistema saranno incaricati mediante opportuna lettera di nomina e relativo mansionario.

## 5. Accesso al sistema informativo MIC

Le assegnazioni delle *Dotazioni* e l'accesso al Sistema Informativo del MiC sono conferite agli utenti sulla base delle esigenze di servizio.

Contestualmente all'inizio del rapporto di lavoro, o alla data indicata nella richiesta di abilitazione, agli utenti viene attribuita un'utenza nei Domain Controller della struttura.

In funzione delle specifiche esigenze di servizio sono configurabili le abilitazioni relative:

a) alla rete SPC (Sistema Pubblico di Connettività);

b) alla casella di posta elettronica personale;

c) ai file server relativi alle cartelle personali;

d) ai file server relativi alle cartelle di servizio;

e) ai software applicativi.

Di norma per gli utenti sono configurate le abilitazioni per i servizi di cui ai precedenti punti a), b), c).

Ulteriori abilitazioni avvengono su richiesta dal dirigente del servizio.

## 6. Attività conduzione sistemi

Gli Amministratori di sistema[3], incaricati dal Ministero e/o appartenenti alle Società appaltatrici per i servizi di conduzione dei sistemi informatici del MiC (gestione postazioni di lavoro, LAN Management, System Management, ecc…) e/o per i servizi di connettività e sicurezza nell'ambito del sistema informatico sono autorizzati a compiere interventi diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per

[3] Nominati ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2007, recante "*Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" come modificato dal provvedimento del 25 giugno 2009.

ulteriori interventi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.…).

Nel rispetto del principio di *minimizzazione dei dati*[4], si prevede che i controlli sull'uso degli strumenti elettronici siano prioritariamente **di tipo aggregato e in formato anonimo**, riferiti all'intera struttura lavorativa del Ministero o a specifici Uffici.

Controlli su base individuale sono giustificabili solo qualora le anomalie, risultando persistenti, costituiscano un pericolo per la sicurezza del sistema e/o per il regolare svolgimento dell'attività d'ufficio e/o qualora l'utilizzo anomalo degli strumenti elettronici rilevato in sede di controllo possa integrare eventuali fattispecie di responsabilità sotto il profilo disciplinare, amministrativo-contabile, civile e/o penale.

Gli Amministratori di sistema hanno la facoltà di collegarsi e visualizzare da remoto il desktop delle singole postazioni di personal computer al fine di garantire l'assistenza tecnica e la normale attività operativa (nonché la massima sicurezza contro i *virus*, *spyware*, *malware*, etc) previa comunicazione e contestuale accettazione dell'intervento da parte dell'utente interessato. Di tali connessioni debbono essere conservati i log di accesso. È in ogni caso fatto divieto di effettuare controlli prolungati, costanti o indiscriminati sull'uso da parte dei lavoratori della dotazione informatica del MiC.

## 7. Direttive sulla Rete Internet

La navigazione in Internet costituisce uno strumento di lavoro e pertanto è utilizzabile esclusivamente per finalità di servizio, fatti salvi i casi in cui risulti consentito l'uso di internet per l'assolvimento di incombenze amministrative o burocratiche del dipendente. Nel riconoscere l'utilità dell'informazione elettronica come mezzo di soddisfacimento delle esigenze informative, formative, culturali e di comunicazione è consentito l'accesso ad Internet anche per uso personale in via saltuaria e del tutto occasionale.

In questo senso, e a titolo non esaustivo, l'Utente non può utilizzare Internet per:

- l'upload o il download di software gratuiti freeware e shareware, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione. In caso di dubbio, il dipendente è tenuto a contattare il personale ICT operante presso la Struttura competente per le verifiche del caso.
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa, sia che ciò avvenga utilizzando email personali sia attraverso l'utilizzo degli account di posta istituzionale;
- la partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guestbooks (libro degli ospiti), anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati;
- porre in essere attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- utilizzare sistemi *Peer to Peer* (P2P), di file *sharing* (condivisione di file all'interno di una rete comune), *podcasting* (sistema che permette di scaricare in modo automatico documenti, generalmente audio o video) o similari, così come connettersi a siti che trasmettono programmi in *streaming* (come radio o TV via Web). Vengono fatti salvi casi eccezionali in cui, per specifiche e motivate ragioni istituzionali e di servizio, detta autorizzazione venga formalmente richiesta e motivata al Dirigente Responsabile dell'Ufficio/Direzione del dipendente interessato. In tale ipotesi, l'autorizzazione è

[4] Considerando n. 39 e articolo 5 comma 1 lett. c) del Regolamento (UE) 2016/679 - Regolamento generale sulla protezione dei dati.

appositamente rilasciata dalla Struttura competente per la gestione dei Sistemi Informativi del MiC, previa opportuna verifica della compatibilità dell'attività richiesta con le complessive esigenze di sicurezza e di funzionamento della rete informatica.

È altresì vietato utilizzare *internet provider* diversi da quello ufficiale del MiC e la connessione delle postazioni di lavoro alle reti di tali *provider* con i sistemi di connessione diversi da quello centralizzato. Vengono fatti salvi casi eccezionali in cui, per specifiche e motivate ragioni istituzionali e di servizio, detta autorizzazione venga formalmente richiesta e motivata al Dirigente Responsabile dell'Ufficio/Direzione del dipendente interessato. In tale ipotesi, l'autorizzazione è appositamente rilasciata dalla Struttura competente per la gestione dei Sistemi Informativi del MiC, previa opportuna verifica della compatibilità dell'attività richiesta con le complessive esigenze di sicurezza e di funzionamento della rete informatica.

Al fine di minimizzare i rischi connessi alla navigazione in siti non pertinenti all'attività lavorativa, il MiC adotta uno specifico sistema di *web filtering* che consente di impostare *policy* in base ai tipi di file, ai protocolli, agli utenti e ai gruppi.

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate in forma elettronica, attraverso i Log di sistema, che vengono conservati per un periodo pari a 3 mesi. Il trattamento dei dati contenuti nei file di log può avvenire esclusivamente in forma aggregata e anonima in modo tale da precludere l'immediata identificazione degli utenti e/o delle loro attività.

I dati personali contenuti nei *log* possono essere oggetto di trattamento, in via eccezionale, ove venga riscontrata una o più delle seguenti ipotesi:

- per corrispondere ad eventuali specifiche richieste di informazioni da parte dell'Autorità giudiziaria;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiedano un immediato e necessario intervento;
- qualora l'utilizzo anomalo degli strumenti elettronici, nonostante le contromisure adottate dall'Amministrazione, in via anonima o aggregata, per l'eliminazione delle relative cause, risulti tuttavia persistente, costituendo per ciò stesso un pericolo per la sicurezza del sistema e/o per il regolare funzionamento delle attività di ufficio;
- qualora l'utilizzo anomalo degli strumenti elettronici possa integrare fattispecie di responsabilità sotto il profilo disciplinare, amministrativo-contabile, civile e/o penale.

L'eventuale prolungamento dei tempi di conservazione dei dati riveste carattere eccezionale ed è consentito nelle ipotesi sopra descritte esclusivamente per il tempo strettamente necessario a realizzare le predette tassative esigenze e limitatamente alle sole informazioni indispensabili a tali fini.

### a) Accesso ad internet

L'utilizzo della rete è consentito a:

- personale a tempo indeterminato e determinato e dirigenti;
- personale comandato da altre amministrazioni;
- personale a vario titolo presente nell'amministrazione ed espressamente autorizzato all'accesso dal Dirigente responsabile.

### b) Obblighi e facoltà dell'utente

L' accesso ad internet per uso personale deve essere limitato, non prevalente rispetto all'attività lavorativa e deve essere improntato a principi generali di correttezza e responsabilità.

Ferma restando la responsabilità disciplinare, civile, amministrativa e penale dell'utente per i reati informatici connessi all'uso personale dell'accesso ad internet, è proibito:

- modificare, rimuovere o danneggiare le configurazioni del software;
- installare software ed applicazioni con funzione di *anonimizzatore;*
- installare software senza l'autorizzazione della struttura informatica;
- navigare in siti di che presentano forme e/o contenuti di carattere pornografico, pedopornografico oppure osceno, blasfemo o diffamatorio secondo quanto stabilito dalla legislazione vigente;
- navigare in siti di scommesse on line e giocare in borsa;
- connettersi con dispositivi non autorizzati. L'uso di tali sistemi è eccezionalmente consentito esclusivamente per la connessione a particolari siti istituzionali protetti e connessi all'attività lavorativa e solo previa verifica e autorizzazione della struttura informatica.

## 8. Direttive sull'uso della rete interna

La gestione del Sistema Informatico deve essere effettuata dallo staff preposto sotto la responsabilità degli Amministratori di sistema. È vietato collegarsi ad Internet attraverso collegamenti a rischio non approvati dal Servizio Sistemi Informativi.

Gli utenti non sono autorizzati ad effettuare alcuna modifica al Sistema, neppure per quei dispositivi hardware e/o software, che hanno ricevuto in dotazione dal Ministero per svolgere il proprio lavoro.

## 9. Direttive generiche sull'uso delle postazioni informatiche

Tutte le postazioni di lavoro devono essere dotate di uno "*screensaver*" protetto da password, con attivazione automatica allo scadere del periodo di inattività considerato opportuno dagli Amministratori di sistema.

La denominazione di ciascuna postazione dovrà fare riferimento all'utente o alla denominazione dell'unità organizzativa che la utilizza. Sono vietate denominazioni di fantasia e diverse da quelle suggerite.

È vietato installare sulle proprie postazioni software non coperto da regolare licenza ed è vietato, altresì, effettuare download di musica, film, e altre opere coperte da diritto d'autore.

Gli utenti sono responsabili per la protezione e tutela delle postazioni informatiche a cui fanno riferimento e dei dati in esse contenuti.

### a) Uso dei computer da tavolo

Il computer da tavolo viene fornito e configurato in base alle mansioni lavorative. Esso è posizionato e manutenuto esclusivamente dallo staff preposto sotto la responsabilità degli Amministratori di Sistema. La sua accensione è prevista per il solo periodo lavorativo. L' Utente, anche in caso di allontanamento temporaneo dalla propria postazione di lavoro, dovrà seguire la procedura di "blocco" del personal computer, fermo

restando che al termine della giornata lavorativa il personal computer dovrà essere sempre spento, unitamente alle altre apparecchiature informatiche collegate. Il posizionamento fisico della postazione informatica deve restare invariato, a meno di formale richiesta di spostamento, da inoltrare al consegnatario informatico.

Il computer deve essere utilizzato esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa, la sua buona cura e l'adeguato utilizzo sono responsabilità dell'assegnatario. In caso di malfunzionamenti della postazione, non è permesso in alcun modo di intervenire a soggetti diversi dal personale preposto.

Il personal computer affidato all'utente dall'Amministrazione consente l'accesso alla rete informatica del MiC solo attraverso specifiche credenziali di autenticazione.

È assolutamente vietato l'uso di programmi diversi da quelli ufficialmente installati dal personale abilitato. Eventuali deroghe sono concesse solo per particolari funzioni svolte. In ogni caso, il controllo dell'attività da parte dell'Amministratore di sistema si svolgerà con le medesime modalità per tutti gli utenti. Non è consentita la duplicazione dei programmi per fornirli a terzi o per uso personale al di fuori del MiC.

Sussistendo il pericolo di introdurre virus informatici (di qualunque natura) e/o di alterare le funzionalità di applicazioni software esistenti, ogni utente deve prestare la massima attenzione in caso di eventuale utilizzo di supporti di origine esterna, avvertendo immediatamente il personale incaricato nel caso in cui sia rilevata (o comunque si sospetti) la presenza di virus nel personal computer.

A tal proposito si rammenta che l'inosservanza delle norme relative ad installazione ed uso di software può esporre il MiC a grave responsabilità civile e/o amministrativa connessa alle violazioni della normativa a tutela dei diritti d'autore sul software.

I dati relativi all'accesso alla postazione informatica vengono automaticamente registrati in forma automatizzata e mantenuti per un periodo pari a sei mesi.

I dati personali contenuti nei log possono essere oggetto di trattamento, in via eccezionale, ove venga riscontrata una o più delle seguenti ipotesi:

- necessità di aderire ad eventuali specifiche richieste di informazioni dell'Autorità Giudiziaria;
- motivata richiesta dell'utente assegnatario della postazione di lavoro o titolare delle credenziali di autenticazione per l'accesso alla rete informatica del Ministero;
- necessità dell'Amministrazione connesse a particolari esigenze di sicurezza.

L'eventuale ulteriore prolungamento dei tempi di conservazione dei dati riveste carattere eccezionale ed è consentito esclusivamente per il tempo strettamente necessario a realizzare le predette tassative esigenze e limitatamente alle sole informazioni indispensabili a tali fini.

### b) Uso dei computer portatili, notebook e tablet

Il computer portatile, notebook o tablet viene fornito in dotazione al solo fine dello svolgimento delle mansioni lavorative. Tali dispositivi vengono configurati, installati e manutenuti esclusivamente dallo staff preposto sotto la responsabilità degli Amministratori di Sistema. L'attrezzatura informatica non deve essere lasciata incustodita da parte dell'assegnatario in condizioni di accessibilità e soprattutto a rischio di furto e/o danneggiamento: ad esempio in auto, treno, aeroporto o altri luoghi in condizioni di scarsa sicurezza. La buona cura e l'adeguato utilizzo sono responsabilità dell'assegnatario. In caso di malfunzionamenti non è permesso in alcun modo l'intervento di soggetti diversi dal personale preposto.

### c) Stampanti

L'Ente mette a disposizione dei propri lavoratori apposite macchine stampanti di rete – anche con modalità c.d. multifunzione - che consentono varie operazioni tra cui la copia cartacea di documenti, la scansione e l'invio via mail degli stessi. Non è consentito, se non occasionalmente, l'utilizzo debitamente autorizzato delle stampanti aziendali per fini personali.

È consigliabile che ciascun Istituto provveda ad equipaggiare tali dispositivi con tecnologie di autenticazione, in modo che solo ed esclusivamente il personale autorizzato possa prelevare la documentazione prodotta, garantendo al contempo una maggiore sicurezza del processo e la riservatezza dei dati trattati.

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

### d) Dispositivi di telefonia fissa

La postazione di lavoro è di norma corredata da un dispositivo di telefonia fissa. Le assegnazioni di linee telefoniche, utenze, apparati e abilitazioni, vengono attribuite dai Sistemi informativi, sulla base di motivate esigenze espresse dagli utenti, previa approvazione del Dirigente/Responsabile.

### e) Telefoni cellulari (smartphone)

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

Tali dispositivi devono essere utilizzati per scopi istituzionali, ad eccezione degli smartphone a uso misto. Nell'ipotesi in cui occorra di riconsegnare il dispositivo, l'assegnatario provvederà previamente alla cancellazione di eventuali dati personali in esso presenti.

Per motivi di sicurezza, l'accesso a tali dispositivi deve essere subordinato alla digitazione di un codice personale (PIN). Nonostante tali cautele, ove siano inevitabilmente presenti sul dispositivo mobile dati ed informazioni considerate critiche dal dipendente, questi dovrà richiedere l'attivazione - se tecnicamente possibile - della possibilità di blocco del dispositivo e la cancellazione dati da remoto in caso di furto.

Le cautele di cui al presente paragrafo trovano applicazione anche nel caso di utilizzo dei servizi di posta elettronica aziendale sullo smartphone di proprietà del dipendente, ad esclusione del caso in cui si acceda mediante web mail.

### f) Dispositivi di firma digitale (o CNS – Carta nazionale dei servizi)

Il dipendente dell'Amministrazione può utilizzare, se munito ed autorizzato all'uso per esigenze di servizio, lo strumento della firma digitale (ovvero della CNS).

### g) Webcam

Per le lo svolgimento delle attività lavorative le postazioni dei dipendenti possono essere dotate di webcam.

L'utilizzo della webcam, non prevede da parte dell'Amministrazione alcun controllo, né alcuna registrazione dei contenuti delle comunicazioni, ferma restando la responsabilità penale, civile ed amministrativa del dipendente nell'ipotesi di compimento di atti illeciti. È vietato l'utilizzo di webcam per comunicazioni private.

## 10. Utilizzo dei dispositivi e strumenti aziendali da parte di personale esterno all'amministrazione

Tutto il personale esterno (consulenti, professionisti, società etc.) che a vario titolo si trova nella condizione di utilizzare dispositivi e strumenti aziendali dell'Amministrazione è tenuto all'osservanza delle disposizioni impartite al personale interno.

Qualora vengano invece utilizzati dispositivi e strumenti propri che si interfacciano con la rete dell'Amministrazione, gli stessi dovranno essere espressamente autorizzati e dovranno essere equipaggiati di tutti i software di sicurezza (antivirus, firewall, aggiornamenti del sistema operativo, etc.).

## 11. Direttive sulla memorizzazione delle informazioni

Ad ogni dipendente è resa disponibile una risorsa di rete: questa risorsa, identificata come disco di rete, è assegnata dall'amministratore di sistema per effettuare i salvataggi dei documenti, come meglio specificato nella successiva lettera c) del presente paragrafo.

Altri salvataggi su cartelle diverse da quella indicata non sono garantiti ai fini dell'applicazione delle misure di sicurezza. In caso di indisponibilità della risorsa, l'utente ha il dovere di informare lo staff tecnico preposto.

### a) Protezione dei dati

L'integrità e la disponibilità delle informazioni e dei dati sono garantite solo quando gli stessi sono memorizzati nei file server messi a disposizione dall'Amministrazione, oggetto di sistemi di protezione, monitoraggio e backup. Non è possibile utilizzare i file server come magazzino di dati personali.

Per garantire la sicurezza e la riservatezza dei dati è fatto obbligo agli utenti di mantenere la riservatezza delle proprie credenziali d'accesso alle dotazioni, al sistema informativo nel suo complesso e ai singoli applicativi.

È altresì obbligatorio presidiare l'intero processo di stampa, fotocopia, scansione o trasmissione via fax di documenti, al fine di impedire l'involontaria o accidentale diffusione di dati personali o la perdita di riservatezza sulle informazioni contenute nei documenti stessi. Allo stesso scopo, è dovere degli utenti prelevare immediatamente i fogli riprodotti da stampanti, fotocopiatrici e fax.

### b) Archivi informatici contenenti dati particolari (ex dati sensibili)

In relazione a specifiche funzioni è possibile che vengano acquisiti e detenuti archivi (cartelle) contenenti dati sensibili e/o dati giudiziari. Queste cartelle/sottocartelle non devono mai essere liberamente accessibili ma protette secondo livelli di autenticazione limitati ai soli soggetti autorizzati.

Per evitare che eventuali accessi abusivi dall'esterno possano compromettere la riservatezza di tale documentazione, è necessario che tali archivi siano cifrati (ad es., zippati con password o analoga misura) e, se detenuti in formato cartaceo, custoditi in contenitori chiusi a chiave ed accessibili solo ai soggetti autorizzati.

### c) Sistema di salvataggio dei dati

A tutto il personale che presta, a qualsiasi titolo, la propria attività lavorativa presso l'Amministrazione, vengono assegnati, ove previsto e previa richiesta, spazi di lavoro:

- personali e dedicati, della rete aziendale (file server) mediante cartelle ad accesso esclusivo;
- condivisi tra tutti gli autorizzati all'accesso.

Operare sugli spazi di lavoro sopra descritti e non in locale costituisce una fondamentale regola di cautela, poiché sulle risorse di rete vengono applicate e gestite, centralmente ed automaticamente, specifiche politiche di back-up secondo la disciplina tecnica vigente

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

## 12. Sistemi antintrusione

Tutti i server utilizzati dall'Amministrazione sono equipaggiati con specifico antivirus i cui aggiornamenti, a cadenza periodica, sono verificati e distribuiti centralmente attraverso specifiche politiche automatiche.

Su ogni singola postazione di lavoro è inoltre installato un ulteriore antivirus (con aggiornamento automatico giornaliero centralizzato) con funzioni di pianificazione di una scansione completa almeno settimanale su ogni dispositivo.

Tali strumenti si occupano automaticamente:

- della ricerca periodica dei files che consentono al motore antivirus di intercettare i codici maligni;
- dell'installazione e dell'aggiornamento automatico della protezione.

Lo stato degli aggiornamenti e delle eventuali incidenze virali è monitorato centralmente da una o più postazioni, di competenza degli amministratori di sistema.

È vietato alterare, disabilitare o modificare i programmi antivirus sopra descritti.

Nel caso si rilevi l'esistenza di un virus o si riscontri (reindirizzamento di pagine web, messaggi indesiderati, blocco di programmi, rallentamenti, etc.), è fatto obbligo all'utente di segnalare immediatamente il problema ai tecnici che gestiscono l'infrastruttura di sicurezza.

## 13. Utilizzo della posta Elettronica

Il MiC fornisce un servizio di posta elettronica, mettendo a disposizione account di posta elettronica attualmente con dominio **@beniculturali.it** e, successivamente, con dominio **@cultura.gov.it**.

Gli account possono essere:

- **personali** (nome.cognome@beniculturali.it, successivamente nome.cognome@cultura.gov.it), basati sull'identità personale e con accesso esclusivo da parte del diretto interessato;
- **istituto/ufficio, servizio/evento**: (nomeistituto/ufficio/servizio/eventi@beniculturali.it, successivamente nome/istituto/ufficio/servizio/eventi@cultura.gov.it), con accesso condiviso tra più utenti della stessa Struttura Organizzativa, individuati dal relativo responsabile. Quest'ultimo definisce e condivide all'interno della struttura le regole di gestione della e-mail, in modo da garantire la continuità ed operatività del servizio e, contestualmente, i principi di stretta necessità e di non eccedenza nel trattamento dei dati. Le denominazioni vengono definite dagli Amministratori centrali su proposta degli Amministratori locali al fine di evitare ripetizioni, ambiguità e confusioni. Il servizio di posta elettronica è uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali. Gli utenti assegnatari delle caselle di posta istituzionale sono responsabili del corretto utilizzo della stessa. Il database di posta elettronica è di

esclusiva proprietà dell'Ente e il personale del CED non può accedere al suo contenuto, nel rispetto della normativa vigente.

### Regole di Utilizzo

Per l'uso del servizio di posta elettronica si applicano le seguenti regole:

- l'uso della posta elettronica aziendale è consentito esclusivamente per motivi attinenti allo svolgimento delle mansioni assegnate. L'utente del servizio è consapevole che i contenuti della posta elettronica dell'Ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa. A puro titolo esemplificativo, è fatto divieto di:
  - sottoscrizione ai social network a titolo personale, partecipazione a dibattiti, forum o mailing-list, newsletter, ed in generale all'uso dei servizi on-line non pertinenti all'attività lavorativa;
  - divulgazione di materiale che violi la dignità e riservatezza di eventuali interessati, ovvero che violi diritti di proprietà intellettuale di terzi;
  - allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro);
  - usare volontariamente il proprio indirizzo di posta elettronica per azioni indiscriminate di "mailing spamming";
  - utilizzare la casella di posta di servizio per attività palesemente incoerenti con la prestazione lavorativa e/o potenzialmente rischiose per la sicurezza della rete informatica.
- è illecito scambiare messaggi sotto falsa identità;
- dato il carattere istituzionale delle caselle di posta del MiC, è fatto divieto d'inoltrare all'esterno messaggi non inerenti alle proprie competenze nell'Ente ed utilizzare l'indirizzo di posta per motivi non legati all'attività lavorativa ed istituzionale;
- è necessario porre particolare attenzione:
  - nel cambiare la password del proprio account di posta almeno ogni tre mesi. La password deve essere modificata solo dal diretto interessato;
  - nel non divulgare a terzi la password dell'account di posta elettronica utilizzata;
  - nell'aprire allegati compressi o contenenti programmi "eseguibili", effettuando sempre un controllo antivirus preventivo su di essi;
  - alla ricezione d'informazioni indesiderate o invasive (c.d. "spam"), pubblicità non istituzionale, manifesta o occulta e comunicazioni commerciali private, di cui non si conosce il mittente. Tali comunicazioni non devono essere aperte e vanno prontamente cancellate. Si precisa inoltre che non bisogna mai rispondere a tali mail poiché si potrebbe incorrere nel rischio di aprire un varco a potenziali pericoli (*virus*, *worm*, *trojan*, etc.), ovvero semplicemente confermare l'esistenza dell'email ai fini dell'inserimento nelle liste di spam;
  - cancellando le mail che invitano alla condivisione di dati personali e/o finanziari (c.d. phishing) o dal dubbio contenuto. Della ricezione di messaggi di tale tipo, deve essere fornita immediata comunicazione al gestore del servizio di posta elettronica della Struttura di appartenenza.
- il titolare di indirizzo di posta elettronica ha il dovere di controllare periodicamente il proprio account di posta elettronica, verificare l'arrivo di nuovi messaggi, cancellare i messaggi obsoleti o inutili,

verificare lo spazio occupato, prestare attenzione ai messaggi di quota raggiunta, ripulire la casella di posta prima del raggiungimento della quota massima consentita;
- al fine di sfruttare razionalmente lo spazio disponibile per la memorizzazione, ogni utente è soggetto a limiti di utilizzo. Il sistema avvisa l'utente all'approssimarsi del raggiungimento della quota limite impostata. Quando la quota viene superata non è più possibile inviare o ricevere messaggi fino a quando non viene liberato spazio sufficiente;
- è opportuno limitare la dimensione dei messaggi inviati, soprattutto nel caso di destinatari multipli. Un allegato di grandi dimensioni potrebbe impedire il corretto smistamento del messaggio o richiedere un uso eccessivo delle risorse, oltre ad essere potenzialmente identificabile come SPAM con il rischio di inserimento dell'account istituzionale in blacklist;
- qualora sia necessario ricevere o spedire documenti di dimensioni maggiori del normale, è necessario utilizzare altri strumenti messi a disposizione dall'Amministrazione (ad esempio ApeCargo);
- è richiesto, nei messaggi in uscita, riportare in calce la firma del soggetto mittente contenente, al minimo: nome, cognome, recapito telefonico ed Ufficio/Servizio di appartenenza;
- poiché la posta elettronica diretta all'esterno della rete del MiC può essere intercettata da estranei, l'invio, tramite tale mezzo, di documenti di lavoro "strettamente riservati" è sconsigliato e comunque va valutato con particolare attenzione;
- in caso di assenza prolungata programmata del dipendente, si consiglia e si raccomanda di attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, l'indirizzo di un collega o del Servizio/Ufficio di riferimento che può essere contattato in sua assenza;
- entro 30 giorni dalla cessazione dell'attività lavorativa presso il MiC, l'account di posta elettronica del dipendente o collaboratore esterno viene disattivato, per essere poi definitivamente cancellato entro 120 giorni.

Ove siano attivi, dopo il pensionamento, incarichi di collaborazione ufficialmente documentati con chiara indicazione del tipo di contratto/accordo e durata dello stesso, potrà essere valutato il mantenimento dell'account di posta elettronica del MiC, che andrà disattivato entro 30 giorni e cancellato entro 120 giorni dal termine della collaborazione. La richiesta di mantenimento dell'account deve essere espressamente motivata.

Prima della cessazione dal servizio a qualsiasi titolo è opportuno, come regola generale, salvare su client locale di posta elettronica e/o inoltrare ad altri, i messaggi che fossero necessari per le successive esigenze lavorative dell'Ufficio nel rispetto, ovviamente, delle regole della privacy.

## 14. Sanzioni

Gli utenti sono direttamente responsabili sia civilmente, sia penalmente, a norma delle leggi vigenti, per l'uso improprio fatto del servizio di internet e della posta elettronica.

L'Amministrazione si riserva la facoltà di denunciare l'utente alle autorità competenti per le attività illecite compiute durante l'attività lavorativa o con i mezzi messi a disposizione dall'Amministrazione.

Per comportamenti non conformi alle presenti linee guida ed agli eventuali Regolamenti applicativi l'Amministrazione si riserva la facoltà di limitare o annullare i privilegi concessi al singolo dipendente.

L'utente è tenuto a risarcire l'Amministrazione per danni prodotti alle apparecchiature o alla rete in violazione delle norme vigenti e/o in violazione del presente disciplinare.

## 15. Controlli

L'Amministrazione adotta misure in grado di prevenire il rischio di utilizzi impropri così da ridurre il più possibile controlli successivi sugli utenti, a garanzia del rispetto della riservatezza delle informazioni e dei dati personali.

### a) Possibilità di controlli e loro gradualità

Il MiC ha diritto di effettuare controlli identificativi degli utenti, quando ciò sia dettato:

- da esigenze per l'esercizio o la difesa in sede giudiziaria;
- da riscontri di gravi inadempienze della prestazione lavorativa;
- da oggettivi indizi di commissione del reato;
- da esigenze di salvaguardia della vita o dell'incolumità di terzi;
- da norme specifiche di legge;
- su richiesta dell'autorità giudiziaria.

Inoltre, le esigenze organizzative, di sicurezza ed il mancato rispetto delle presenti direttive che evidenzino comportamenti anomali (evento dannoso, situazione di pericolo, rischi di responsabilità per l'ente, interferenze, rischio o danno per altri), legittimano il Ministero al controllo sull'utilizzo del web e dell'e-mail. La verifica sui comportamenti anomali verrà effettuata con controllo preliminare su dati aggregati e anonimi, riferiti all'intera struttura lavorativa del Ministero o a specifici Uffici.

Il controllo anonimo può concludersi con avviso generalizzato sul rilevato utilizzo anomalo degli strumenti dell'ente e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle disposizioni impartite. L'avviso e l'invito verranno rivolti solo alla Struttura/Ufficio in cui verrà eventualmente rilevata l'anomalia.

In assenza di successive anomalie non saranno effettuati controlli individuali.

Non possono essere effettuati controlli prolungati, costanti o indiscriminati.

### b) Conservazione dei dati

Vengono conservati per un periodo pari a 6 mesi i log di accesso relativi all'uso degli strumenti elettronici indispensabili per le seguenti finalità:

- protezione dell'intera rete da e verso l'esterno (firewall);
- difesa della corrispondenza e navigazione informatica (antispamming/antivirus);
- controllo automatico dei contenuti dei siti (web filtering).

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad Internet e al traffico telematico.

Eccezionalmente la conservazione può essere ulteriormente protratta, per il tempo indispensabile e per le sole informazioni necessarie, in relazione:

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

Il Responsabile per la sicurezza informatica, in collaborazione con il Responsabile del CED, conformandosi ai principi di necessità, correttezza, pertinenza e non eccedenza di cui al Regolamento (UE) 2016/679, potrà provvedere al controllo delle informazioni relative ai dati sopra descritti.

Per la verifica del corretto utilizzo della posta elettronica ed internet:

- si riserva la facoltà di effettuare controlli periodici nei log file, in conformità della legge e al solo fine di garantire la funzionalità e sicurezza del sistema. I dati da elaborare verranno estratti in forma anonimizzata, privi di qualsiasi riferimento che possa essere ricondotto all'utente (matricola, cognome nome, indirizzo IP, MAC Address);
- elabora informazioni di tipo statistico quali accessi a banche dati e visite a siti di interesse, riservandosi la facoltà di raggruppare dati per struttura per verifiche di fruibilità;
- non effettua monitoraggi sistematici delle pagine Web visualizzate dal singolo lavoratore. Saltuariamente può estrarre pagine visitate dai dipendenti, prive di riferimenti che possano essere ricondotti al singolo utente, per l'individuazione di siti non correlati all'attività lavorativa, da inserire nel *web filtering*.

L'attività di monitoraggio viene svolta dal Responsabile per la sicurezza informatica in collaborazione con gli uffici preposti a questi servizi, nel rispetto del principio di riservatezza di cui all'art. 5, par. 1, lett f) del GDPR.