DISCIPLINARE INTERNO SULLE NORME COMPORTAMENTALI PER L'ACCESSO AI SISTEMI ED ALLE RISORSE INFORMATICHE, PER LA GESTIONE DELLA NAVIGAZIONE IN INTERNET E DELLA POSTA ELETTRONICA DELL'ISTITUTO NONCHÈ DELLA GESTIONE DEI DOCUMENTI ANALOGICI.

Il presente documento ha per oggetto i criteri e le modalità operative per l'accesso ai sistemi ed alle risorse informatiche, per la gestione della navigazione in Internet e della posta elettronica da parte dei dipendenti dell'Istituto e di tutti gli altri soggetti autorizzati che, a vario titolo, prestano servizio o attività per conto e nelle strutture aziendali.

Di seguito, vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte, che anche inconsapevolmente, potrebbero comportare rischi alla sicurezza dei dati, documenti e archivi.

1. UTILIZZO DELLE POSTAZIONI DI LAVORO, SISTEMI PORTATILI, STAMPANTI

1.1 La postazione di lavoro affidata al dipendente deve essere utilizzata strettamente per attività lavorative ed ogni utilizzo differente può contribuire a creare dei disservizi; inoltre, potrebbe insinuare minacce alla sicurezza dei Dati trattati da ICCD. Tutti i dipendenti devono custodire la propria postazione di lavoro in modo diligente, segnalando per tempo ogni anomalia riscontrata e/o guasto all'indirizzo email ic-cd.assistenzainformatica@beniculturali.it.

1.2 L'accesso a ciascuna postazione è protetto da credenziali di autenticazione che risiedono sul Server di Dominio: tali credenziali sono costituite da "userID" e "password", e sono conosciute esclusivamente dall'utente.

1.3 Le credenziali di autenticazione devono essere gestite attenendosi alle seguenti istruzioni:

1.3.1 La password deve essere costituita da almeno otto caratteri alfanumerici di cui almeno tre differenti (scelti tra lettere minuscole, maiuscole e numeri).

1.3.2 La password deve essere autonomamente sostituita dall'utente (policy impostata lato Server di Dominio) al primo utilizzo e successivamente modificata ogni qual volta sia richiesto dal sistema.

1.3.3 La password non deve contenere riferimenti diretti o indiretti agevolmente riconducibili all'utente stesso.

1.3.4 Le password (anche quelle degli applicativi, i PIN e/o qualsiasi altro codice di protezione) devono essere custodite con la massima attenzione e segretezza (non devono mai essere scritte su fogli o biglietti che vengono lasciati in prossimità del PC) e

non devono essere divulgate o comunicate a terzi per nessuna ragione. Saranno passibili di provvedimenti i metodi "non standard" quali post-it, calendari e qualsiasi altro mezzo non idoneo di custodia, che potrà creare un uso illecito delle credenziali.

1.3.5 L'utente è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.

1.3.6 Le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise con altri utenti. Se un utente necessita di trattare gli stessi Dati e/o le stesse procedure dovrà richiedere, delle credenziali personali.

1.3.7 È fatto divieto di comunicare la password per telefono o altro mezzo a soggetti che si presentano come colleghi, tecnici e supervisori.

1.4 Il dipendente preso atto che, la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai Dati cui il medesimo è abilitato, con possibilità di gestione degli stessi, si impegna a:

1.4.1 non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;

1.4.2 non utilizzare credenziali (user ID e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti a conoscenza casualmente;

1.4.3 mantenere la corretta configurazione del proprio PC non alterando le componenti hardware e software predisposte, né tanto meno installando dei software non autorizzati.

1.5 Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

1.6 Non rispondere a messaggi di posta elettronica che richiedano la verifica delle proprie credenziali di accesso ai servizi finanziari (banche o altri istituti finanziari).

1.7 Ogni postazione di lavoro dovrà essere bloccata in caso di non utilizzo o di assenza temporanea, tramite la chiusura della sessione di lavoro sul pc facendo logout oppure, in alternativa, attivando un salvaschermo con richiesta di password al riavvio. Sarà compito del dipendente procedere a tale blocco.

1.8 Si ricorda che il salvaschermo: non deve mai essere disattivato; deve essere messo in funzione manualmente ogni volta che si lascia il pc acceso ed incustodito.

1.9 In caso di assenza prolungata nel corso della giornata, è fatto obbligo di chiudere le applicazioni aperte dalle quali si ha accesso ai dati personali.

1.10 Spegnere sempre la propria postazione e i relativi dispositivi ad essa connessi al termine dell'orario di lavoro.

1.11 Non è consentito installare/eseguire autonomamente software provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del Servizio Informatico.

1.12 Non è consentito ai dipendenti modificare le impostazioni sulla scheda di rete LAN e neppure sul browser di navigazione, salvo esplicita autorizzazione del Responsabile del Servizio Informatico.

1.13 Non è assolutamente consentito l'uso/l'installazione sul proprio PC di dispositivi, neanche personali, di memorizzazione (HardDisk Esterni, chiavette USB, ecc), comunicazione o altro (masterizzatore, ecc) se non previa espressa autorizzazione del Responsabile del Servizio, dopo richiesta scritta da parte del soggetto cui è assegnato l'elaboratore.

1.14 In caso di autorizzazione all'utilizzo di supporti di memorizzazione, gli stessi dovranno essere di proprietà del Titolare ed andranno criptati.

1.15 Ogni dipendente deve comunque prestare la massima attenzione ai supporti di memorizzazione di origine esterna onde evitare di scaricare, anche inconsapevolmente, virus e/o qualunque codice maligno.

1.16 È assolutamente vietato copiare, scaricare e mettere a disposizione di altri materiale protetto da copyright (files musicali, filmati, ecc) di cui il Titolare non abbia acquisito i diritti.

1.17 In caso di utilizzo di dispositivi di proprietà del dipendente che conservano documenti di lavoro, si richiede che anche questi vengano protetti ed in caso di smarrimento/vendita o altra perdita di possesso, si avvisi preventivamente o tempestivamente (entro 24 ore), in forma scritta, il direttore dell'Istituto.

1.18 Le stampanti verranno installate per gruppi di lavoro, tramite policy di dominio. Per finalizzare la procedura di stampa, andrà inserito un PIN personale al momento del ritiro dei fogli stampati.

1.19 Gli scanner potranno essere configurati per poter scansionare in cartelle di rete, legate ai gruppi di lavoro. Sarà cura dell'utente cancellare, dalla cartella condivisa, i documenti scansionati una volta verificata l'attività di scansione.

2. DOCUMENTI INFORMATICI

2.1 I documenti di lavoro andranno salvati esclusivamente negli archivi messi a disposizione da ICCD (file server, cartelle condivise e/o software gestionali).

2.2 Il contenuto della postazione di lavoro è di accesso esclusivo dell'utente. In caso di assenza del dipendente, sarà possibile ai soli Amministratori di Sistema accedere al contenuto dell'elaboratore. In questo caso, l'utente verrà informato dell'avvenuto accesso.

2.3 In ogni caso, non sono ammessi documenti di tipo personale, di qualsivoglia formato (foto, video, ecc). ICCD non è responsabile della perdita/alterazione dei suddetti dati se conservati sui propri sistemi.

2.4 Non è consentito l'uso di "cloud", se non espressamente autorizzati dal dall'Amministratore di sistema, previa verifica di adeguatezza alla normativa vigente. Di default questi servizi vengono inseriti in "Black List" (vedi ARTICOLO 3).

2.5 Il dipendente che conserva i documenti informatici sul proprio computer e non nel file server messo a disposizione, è direttamente responsabile della loro perdita per eventuali guasti dell'elaboratore.

3. NAVIGAZIONE IN INTERNET

3.1 La postazione collegata ad Internet costituisce uno strumento necessario allo svolgimento dell'attività lavorativa, di conseguenza è proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

3.2 Al fine di prevenire rischi di utilizzo improprio della rete reputati non compatibili con l'attività lavorativa sono utilizzati sistemi di filtri che impediscono l'accesso diretto a siti non in linea con le finalità di ICCD (black list); questa viene progressivamente implementata e completata.

3.3 Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta e delle informazioni che vi immette. È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo i casi espressamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure assegnate.

3.4 È vietata ogni forma di registrazione a siti o mailing list i cui contenuti non siano legati allo svolgimento delle attività lavorative assegnate.

3.5 È vietata la navigazione di siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche o le abitudini sessuali dell'utilizzatore; non è consentito, inoltre, visitare nè tanto meno memorizzare documenti dal contenuto oltraggioso, discriminatorio che offendono il comune senso del pudore.

3.6 Qualora il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario darne immediatamente segnalazione all'Amministratore di sistema alla email ic-cd.assistenzainfromatica@beniculturali.it. .

3.7 Non inserire i propri dati di login cliccando direttamente sui link proposti all'interno di un'email, ma digitare l'indirizzo del sito manualmente per essere certi di non incorrere in siti contraffatti (es. phishing).

3.8 Non cancellare la sottoscrizione ad una mailing list di cui non si è certi dell'iscrizione (potrebbe trattarsi di un raggiro da parte di uno spammer per ottenere conferme sulla validità dell'indirizzo email dell'utente).

3.9 I log di sistema debbono essere conservati per non più di 180 giorni e possono essere resi disponibili esclusivamente sulla base della normativa vigente.

4. GESTIONE DELLA POSTA ELETTRONICA, PEC E FIRMA DIGITALE

4.1 L'utilizzo della posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Titolare assegna una casella email di posta personale e/o di servizio.

4.2 La casella di posta messa a disposizione da ICCD è uno strumento di lavoro che deve essere quindi utilizzato esclusivamente per esigenze connesse all'attività lavorativa. Non sono ammessi utilizzi diversi o privati dell'indirizzo; conseguentemente i dipendenti ai quali è assegnata sono responsabili del corretto utilizzo della stessa.

4.3 Si evidenzia che, nel caso di trasmissione di dati particolari (art. 9 GDPR) e/o giudiziari (art. 10 GDPR), è opportuno fare ricorso alla crittografia dei documenti.

4.4 È assolutamente vietato:

a. l'utilizzo di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti all'attività svolta per ICCD;

b. inoltrare catene telematiche (es. petizioni, giochi) e altre forme di email che non abbiano attinenza con l'attività svolta;

c. utilizzare tecniche di "mail spamming", invio massiccio di comunicazioni a liste di utenti non istituzionali;

d. allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi eseguibili, macro, script ecc.).

4.5 L'Istituto provvederà a mettere a disposizione di ciascun dipendente apposite funzionalità di sistema, che consentano di inviare automaticamente, in caso di assenza dal servizio dell'utente, messaggi di risposta che avvisino il mittente dell'assenza del destinatario, indicandogli, altresì, le coordinate di un altro lavoratore autorizzato a leggere le comunicazioni durante l'assenza.

4.6 Dopo la cessazione del rapporto di lavoro, l'account sarà rimosso previa disattivazione. L'account verrà disattivato decorsi sessanta giorni dalla cessazione del rapporto: tale periodo servirà ad informare i terzi e a fornire a questi ultimi degli indirizzi alternativi cui rivolgersi per restare in contatto con gli Uffici del Titolare competenti per gli specifici procedimenti/affari.

4.7 In caso di utilizzo di dispositivi personali per l'accesso alla posta elettronica, si richiede che anche questi vengano protetti (es: pin, blocco schermo sequenza, sistemi biometrici) e in

caso di smarrimento/vendita o altra perdita di possesso, si avvisi preventivamente o tempestivamente (entro 24 ore), in forma scritta, l'Amministratore di Sistema.

4.8 Nel caso di mittenti sospetti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

4.9 Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

4.10 L'Istituto si è dotato di Posta Elettronica Certificata a disposizione dei vari uffici. L'utilizzo di altre PEC non istituzionali non è consentito.

5. DOCUMENTI ANALOGICI (cartecei)

5.1 Il dipendente non dovrà lasciare incustoditi i documenti contenenti dati personali a lui affidati per l'esercizio della sua attività.

5.2 Il dipendente dovrà evitare il deposito di questi documenti in luoghi di transito come corridoi o sale riunioni.

5.3 I documenti in entrata e in uscita contenenti dati personali debbono essere consegnati dalla segreteria direttamente al servizio interessato, e viceversa.

5.3 Se la persona designata al trattamento dei dati è costretta ad allontanarsi momentaneamente non deve mai lasciare incustoditi i documenti e gli atti contenenti dati personali e sensibili sulle scrivanie o in altro luogo liberamente accessibile a terzi non autorizzati.

5.4 L'incuria può essere causa di sottrazione di documenti contenenti dati personali o istituzionali con conseguente possibile trattamento illecito; il dipendente è perciò tenuto a rispettare quanto di seguito indicato:

i. al termine della sessione di lavoro ricollocare i documenti negli appositi cassetti e contenitori evitando di mantenerli a vista sulla postazione assegnata per tutta la durata dell'assenza;

ii. usare promemoria volanti solo per indicazioni generiche;

iii. distruggere i dati cartacei contenenti dati sensibili qualora non debbano essere più utilizzati (es. mediante una tritadocumenti);

iv. qualora, per la mansione assegnata, il dipendente tratti abitualmente atti o documenti contenenti dati sensibili dovrà custodirli in armadi chiusi a chiave all'interno di uffici dotati di idonee misure di sicurezza. L'accesso a tali documenti sarà monitorato e consentito solo a coloro che ne sono stati espressamente autorizzati dal loro responsabile;

v. qualora, per la mansione assegnata, il dipendente tratti solo accidentalmente atti o documenti contenenti dati sensibili detti dati dovranno essere dallo stesso controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e dovranno essere immediatamente restituiti al termine delle operazioni affidate.

5.5 È severamente vietato utilizzare documenti contenenti dati personali, particolari o giudiziari come carta da riciclo o carta per appunti. Anche al fine di riduzione dei costi, è pertanto opportuno che – in caso di stampa di documenti – i dipendenti utilizzino la modalità "fronte/retro".

5.6 L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

6. ULTERIORI MISURE ORGANIZZATIVE

Con riferimento alle principali operazioni delle persone autorizzate al trattamento si specifica quanto segue:

6.1 Identificazione dell'interessato: al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni.

6.2 Verifica del controllo dell'esattezza del dato e della corretta digitazione: al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

6.3 Norme logistiche per l'accesso fisico ai locali: i locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di dati personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario

lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali.

6.4 Rilevazione presenze: ICCD è dotato di un servizio di rilevazione delle presenze e di un servizio di reception/sorveglianza. In questo caso, ogni incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

GLOSSARIO

Black List: elenco di siti internet non accessibili da parte degli utenti della rete locale.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dato particolare: l'art. 9 GDPR definisce come particolari tutti quei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

GDPR: acronimo di General Data Protection Regulation (in italiano "Regolamento generale sulla protezione dei dati") adottato dal Parlamento europeo e dal Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi, divenuto pienamente applicabile il 25 maggio 2018.

Incaricati del trattamento dei Dati: non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice), il Regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4, par. 10, Reg. UE 2016/679 (GDPR), definizione di «terzo»).

Log: archivio dei tracciati sulle attività di consultazione in rete locale e non.

Postazione di Lavoro: personal computer collegato alla rete locale tramite la quale l'utente accede ai Servizi ed ai Dati da gestire.

Responsabile del trattamento dei Dati: secondo quanto elencato nell'art. 4, par. 8, Reg. UE 2016/679 (GDPR), per responsabile del trattamento si intende "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". Nel caso dell'ICCD il responsabile del trattamento dei dati personali è la Direzione generale Educazione e ricerca.

Sistemi Portatili: notebook, smartphones e tablet.

Titolare del trattamento: secondo quanto previsto dall'art.4, par. 7, Reg. UE 2016/679 (GDPR) "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali". Il Titolare è il Ministero per i beni le attività culturali.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Utente e-mail (posta elettronica): persona autorizzata ad accedere al servizio di posta elettronica attraverso l'utilizzo di caselle email.

Utente Internet: persona autorizzata ad accedere al servizio di navigazione in Internet.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Aggiornamento: agosto 2018