Agenzia per la Coesione Territoriale

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Sommario

1. Introduzione

1.1. Scopo del documento e criteri generali

Il presente Disciplinare Interno, conformemente a quanto stabilito dalla normativa vigente in relazione all'uso degli strumenti informatici e dal "Codice di comportamento e di tutela della dignità e dell'etica" dell'Agenzia per la Coesione Territoriale, ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme nell'utilizzo di tali strumenti da parte degli utenti, al fine di evitare che condotte inconsapevoli o scorrette possano esporre l'Amministrazione a problematiche di sicurezza, di immagine oltre che patrimoniali per possibili danni cagionati a terzi, e i singoli utenti ad eventuali responsabilità disciplinari o penali. In particolare, è necessario garantire:

- la protezione dell'Amministrazione da atti illeciti attuati mediante l'uso delle dotazioni informatiche;
- la prevenzione dei reati di criminalità informatica (D. Lgs. 231/2001);
- la sicurezza delle informazioni in termini di disponibilità, integrità e riservatezza;
- l'impiego efficiente ed efficace delle risorse affidate;
- l'adozione di una disciplina conforme alle disposizioni del Garante per la protezione dei dati personali (Garante Privacy) ed il rispetto delle leggi vigenti in materia;
- una corretta informativa sulle modalità d'uso degli strumenti.

L'Amministrazione mette a disposizione del personale, interno ed esterno, che opera nell'ambito del mandato istituzionale dell'Agenzia per la Coesione Territoriale, i seguenti strumenti e servizi informatici, necessari allo svolgimento delle attività lavorative, in funzione del ruolo e delle esigenze di ciascuno:

- Personal Computer (PC) installati sul posto di lavoro, computer e altri dispositivi portatili, stampanti e scanner individuali o di rete;
- servizi di posta elettronica e Internet;
- servizi applicativi e software generalizzato.

Tali risorse costituiscono strumenti di lavoro e devono pertanto essere utilizzate per il perseguimento di fini strettamente connessi agli incarichi lavorativi, secondo criteri di massima

correttezza e professionalità, coerentemente al tipo di attività svolta e in linea con le disposizioni normative vigenti. L'utente è direttamente responsabile del corretto uso di tali risorse.

L'Amministrazione si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali vigenti, il rispetto delle presenti disposizioni al fine di garantire l'integrità, la sicurezza e l'efficienza del proprio Sistema Informativo. Si precisa che tali verifiche non sono finalizzate al controllo dell'attività lavorativa degli utenti, e che i dati registrati dai sistemi non devono in alcun modo ritenersi utilizzabili per il controllo a distanza dei lavoratori.

1.2. Responsabile del documento e della sua diffusione

Responsabile dell'elaborazione e dell'aggiornamento periodico del presente documento è l'Ufficio 3 di Staff - Sistemi informativi e Acquisti, in collaborazione con l'Ufficio 2 di Staff - Organizzazione, Bilancio e Personale, che ha la competenza istituzionale dell'organizzazione dell'Agenzia. Lo stesso Ufficio 3 lo renderà disponibile, nella versione più aggiornata, sulla Intranet istituzionale.

Contestualmente alla attivazione delle credenziali di autenticazione, l'utente verrà informato via e-mail dal Supporto Utenza dell'Ufficio 3 di Staff dell'esistenza del "Disciplinare Interno per l'Utilizzo degli Strumenti Informatici", di cui è tenuto a prendere visione.

2. Riferimenti Normativi

Il presente Disciplinare Interno è redatto in conformità alla normativa in materia di protezione dei dati personali, e in particolare alla normativa di seguito riportata e relative successive modifiche e integrazioni.

2.1. Riferimenti interni

- Codice di comportamento e di tutela della dignità e dell'etica dell'Agenzia per la Coesione Territoriale, (Decreto del Direttore Generale n. 14/2017).

2.2. Riferimenti legislativi

- Legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attività sindacale nel luoghi di lavoro e norme sul collocamento" (Statuto dei Lavoratori), con particolare riferimento all'art. 4 che vieta di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori;
- Decreto legislativo 29 dicembre 1992 n. 518 "Attuazione della Direttiva 91/259/CEE relativa alla tutela giuridica dei programmi per elaboratore";
- Legge 23 dicembre 1993 n. 547 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
- Legge 18 agosto 2000 n. 248 contenente "Nuove norme di tutela del diritto d'autore";
- Decreto Legislativo 8 giugno 2001 n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica";
- Decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";
- Direttiva MIT del 27 novembre 2003 per l'"impiego della posta elettronica nelle Pubbliche Amministrazioni";
- "Codice dell'amministrazione digitale" Decreto Legislativo 7 marzo 2005, n. 82;
- Deliberazione del Garante Privacy n. 13 del 1° marzo 2007 "Linee guida del Garante per posta elettronica e Internet";
- Legge 18 marzo 2008 n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno";
- Decreto Legislativo 14 settembre 2015 n. 151 contenente "Disposizioni di razionalizzazione e

semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183" che ha modificato l'articolo 4 della legge 20/05/1970 n. 300;

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- Decreto Legislativo 26 agosto 2016, n. 179 "Modifiche ed integrazioni al Codice dell'amministrazione digitale", di cui al decreto legislativo 7 marzo 2005, n. 82;
- Agenzia per l'Italia Digitale (AGID), circolare 17 marzo 2017, n. 1/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015);
- Art. 15 della Costituzione della Repubblica Italiana, in cui si stabilisce che «La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria, e con le garanzie stabilite dalla legge»;
- Codice Penale art. 616 - Violazione, sottrazione e soppressione di corrispondenza che, a tutela della riservatezza della corrispondenza, "telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza", regolamenta e sanziona l'accesso a tali strumenti.

3. Principi generali di utilizzo degli strumenti informatici

Al personale interno ed esterno che opera nell'ambito del mandato istituzionale dell'Amministrazione, viene assegnata una Postazione di Lavoro (PdL). L'Ufficio 3 di Staff - Sistemi informativi e Acquisti è preposto alla assegnazione delle PdL e di eventuali altre dotazioni informatiche, alla loro gestione e manutenzione sia hardware che software, alla assegnazione, gestione e rigenerazione delle credenziali di autenticazione, e alla gestione, protezione e salvataggio delle aree dati presenti sulle unità di rete condivise.

L'assegnatario della PdL e/o di altre dotazioni informatiche è responsabile dell'integrità e del buon uso della strumentazione ricevuta, il cui utilizzo dovrà avvenire nel rispetto del presente Disciplinare e della normativa di riferimento, con particolare attenzione a quanto specificato nell'art. 2 del Codice di comportamento e di tutela della dignità e dell'etica dell'Agenzia per la Coesione Territoriale.

3.1. Norme nell'utilizzo degli strumenti informatici

Per una corretta gestione dei sistemi informatici, gli utenti devono scrupolosamente attenersi alla regole di seguito riportate, la cui mancata osservanza può determinare il ricorso ad azioni disciplinari.

- I sistemi informatici, fisici e logici, nonché le reti di comunicazione sono strumenti di lavoro, e come tali devono essere usati esclusivamente per lo svolgimento delle mansioni assegnate;
- l'utilizzo degli strumenti informatici deve avvenire nel pieno rispetto dei requisiti di sicurezza, al fine di mantenere elevati livelli di riservatezza, di integrità e di disponibilità delle informazioni;
- tutti i documenti elettronici creati, memorizzati, trasmessi o comunque trattati utilizzando macchine e sistemi pertinenti all'Amministrazione sono di competenza dell'Amministrazione stessa, che può accedervi ogni qualvolta sia necessario per esigenze operative o legali, nel rispetto delle disposizioni dettate in materia di diritto alla privacy, di tutela del lavoratore nonché delle ulteriori regole di segretezza eventualmente applicabili;
- i dati memorizzati in locale sulle PdL assegnate non vengono salvati a cura dell'Ufficio 3 di Staff. Pertanto, è opportuno che l'utente effettui periodicamente copie di sicurezza (backup) dei documenti elettronici considerati essenziali nell'ambito del proprio lavoro, ovvero utilizzi gli spazi messi a disposizione su unità di rete condivise (file sharing) o cartelle allocate su disco Z:

(HomeDir) – di cui viene effettuato il salvataggio periodico a cura dell'Ufficio 3 di Staff – facendo particolare attenzione, per quanto riguarda i documenti contenenti dati personali, sensibili o giudiziari, a quanto previsto dal D. Lgs.196/03;

- in caso di abbandono temporaneo della PdL, gli utenti sono tenuti a proteggere il computer da accessi non verificabili, bloccandone con la funzione apposita l'utilizzo (nel sistema operativo Windows, tramite la combinazione di tasti : Ctrl + Alt + Canc , e quindi "Blocca computer", oppure attivando la funzione automatica di screen saver con password), che potrà essere ripristinato solo mediante la reintroduzione della password. Si sottolinea che lasciare il PC incustodito e accessibile, con la sessione di lavoro attiva, può essere causa di utilizzo da parte di terzi non autorizzati, e ciò ricadrebbe sotto la diretta responsabilità dell'utente;
- al termine dell'attività lavorativa, o in caso di prolungato inutilizzo della postazione, è necessario spegnere il PC e le periferiche locali;
- l'assegnatario, in caso di smarrimento o furto delle dotazioni informatiche assegnategli, deve provvedere immediatamente a sporgere regolare denuncia all'autorità giudiziaria competente, inviandone copia al Dirigente/Responsabile della struttura di riferimento e al Dirigente dell'Ufficio 3 di Staff. Si dovrà inoltre comunicare alle suddette funzioni il tipo di dati eventualmente smarriti o sottratti. Contestualmente, è necessario modificare le eventuali password che si pensa possano essere state violate.

3.2. Limitazioni nell'uso degli strumenti informatici

- Non è consentito smontare, o manomettere le attrezzature informatiche messe a disposizione dall'Amministrazione;
- non è consentito modificare la configurazione hardware o software, né disinstallare il software standard presente sulla propria PdL al momento dell'assegnazione; eventuali giustificate modifiche dovranno essere formalmente autorizzate dal Dirigente/Responsabile della struttura di riferimento e dall'Ufficio 3 di Staff;
- qualora si debba, previa autorizzazione del Dirigente/Responsabile della struttura di riferimento e dell'Ufficio 3 di Staff, installare o aggiornare del software per motivi di servizio, potrebbe essere necessario autenticarsi alla PdL con le credenziali di "amministratore". In questo caso, rivolgersi al Referente Informatico o al Supporto Utenza dell'Ufficio 3 di Staff.
- tutto il software presente sulla PdL deve essere di proprietà dell'Amministrazione o essere da essa autorizzato, e provvisto di adeguata licenza; ne consegue che l'assegnazione della PdL autorizza l'assegnatario all'utilizzo del software installato, le cui licenze sono detenute dall'Amministrazione;
- non è consentita la riproduzione o la duplicazione di programmi software, nel rispetto della normativa vigente in materia di diritto di proprietà intellettuale;
- non sono permessi l'installazione e l'utilizzo di software non attinente alla materia di lavoro di propria pertinenza, né l'uso di software personale, se non esplicitamente autorizzato dal Dirigente/Responsabile della struttura di riferimento e dall'Ufficio 3 di Staff;

- non possono essere utilizzate strumentazioni informatiche personali (supporti di archiviazione rimuovibili o altri dispositivi), non autorizzate, astrattamente idonee ad estrapolare o alterare i dati;
- in ogni caso, non è consentito l'uso di CD-Rom, dispositivi USB o altri supporti di archiviazione removibili di contenuto non verificato che possano arrecare danno alla PdL;
- non è permesso l'uso di dispositivi di connessione con l'esterno, come modem, fax, bluetooth ecc.se non autorizzati dall'Amministrazione;
- non è consentito il collegamento di strumenti informatici non forniti dall'Amministrazione alla rete istituzionale o alla rete wi-fi istituzionale, se non preventivamente autorizzato dal Dirigente/Responsabile della struttura di riferimento e dall'Ufficio 3 di Staff. Anche se autorizzato, l'utente è tenuto ad adeguare il dispositivo alle configurazioni standard e, in ogni caso, ad attenersi alle medesime regole valide per la strumentazione informatica interna;
- non è consentito trasferire o spostare di stanza le attrezzature informatiche fisse senza il diretto coinvolgimento dell'Ufficio 3 di Staff, che opererà d'intesa con il Consegnatario.

4. Gestione delle credenziali di autenticazione

Le credenziali assegnate a ciascun utente sono nominative e strettamente personali, e consentono, mediante un sistema di autenticazione unica, l'accesso al Dominio di rete *"dps.economia.net"*. L'utente è direttamente responsabile del corretto uso delle sue credenziali. L'accesso al Dominio di rete permette l'utilizzo dei vari servizi informatici messi a disposizione, fra cui il file sharing, i servizi di posta elettronica ed Internet.

Le credenziali possono essere concesse esclusivamente a:

- tutto il personale dipendente a tempo indeterminato e determinato, in posizione di comando, distacco o fuori ruolo;
- i componenti del Nucleo di verifica e controllo (NUVEC);
- i collaboratori, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo;
- i componenti degli Organi;
- i collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi o che realizzino opere in favore dell'Agenzia.

Esse vanno richieste da parte del Dirigente/Responsabile della struttura di riferimento dell'utente al Supporto Utenza dell'Ufficio 3 di Staff, che provvederà alla creazione dell'account di Dominio e alla erogazione delle nuove credenziali. L'utente, per motivi di sicurezza, sarà invitato a ritirarle personalmente presso il Supporto Utenza dell'Ufficio 3 di Staff.

Le credenziali sono composte dal nome utente (nome.cognome) e dalla relativa password, che dovrà essere sostituita al primo utilizzo. La password è una sequenza di caratteri conosciuta soltanto all'utente, costruita sulla base delle seguenti regole:

- la lunghezza deve essere non inferiore a 8 caratteri;
- la validità è di durata limitata; essa deve essere sostituita tutte le volte che il sistema di accesso lo richiede. La nuova password dovrà essere diversa dalle ultime 4 utilizzate;
- la definizione non deve includere informazioni facilmente deducibili, quali per esempio il proprio nome o cognome, la data di nascita propria o di un parente, il codice fiscale, ecc.;

- il contenuto deve essere mantenuto riservato, evitandone la trascrizione su supporti accessibili a terzi;
- la segretezza deve essere garantita, provvedendo alla sostituzione qualora la stessa venga meno.

Le password di accesso alla rete e alla posta elettronica sono le medesime; per l'accesso ad altri sistemi o servizi (applicazioni informatiche, siti Internet e social network) devono essere usate password diverse, in modo che la compromissione di una di queste non impatti sulle altre.

Le password per l'accesso via browser alle applicazioni istituzionali non devono mai essere memorizzate sulla PdL attraverso le funzionalità automatiche del software, anche se detta memorizzazione non fosse disattivata per impostazione predefinita.

In caso di oblio o smarrimento delle credenziali di accesso, occorre rivolgersi al Supporto Utenza dell'Ufficio 3 di Staff per il ripristino delle stesse.

Non è consentito accedere al sistema informativo utilizzando le credenziali di accesso altrui e/o comunicare ad altri la password relativa alle proprie credenziali di accesso. Si raccomanda ulteriormente, al fine di ridurre il rischio di utilizzi indebiti, di non scrivere le proprie password su foglietti di carta o in altre modalità facilmente accessibili a terzi.

5. Protezione da virus

Per la salvaguardia dei dati e al fine di garantire il corretto funzionamento della PdL ed evitare di esporre la rete dell'Amministrazione ad attacchi informatici, l'utente deve tenere comportamenti tali da ridurre il rischio di diffusione di virus, che può derivare dalle operazioni di scambio di dati mediante supporti removibili e messaggi di posta elettronica, potenziali veicoli di programmi e file infetti. Anche la navigazione in Internet può esporre al pericolo di diffusione di virus.

Al fine di minimizzare tali rischi per la propria PdL e di evitare di compromettere la sicurezza del Sistema Informativo Istituzionale, è necessario osservare le regole stabilite dall'art. 2 del "Codice di comportamento e di tutela della dignità e dell'etica" dell'Agenzia per la Coesione Territoriale. Inoltre:

- il programma antivirus deve essere installato, aggiornato regolarmente e funzionante su ciascuna PdL. Nel caso di dispositivi solo saltuariamente collegati alla rete istituzionale, come computer portatili o altro, l'utente deve richiedere periodicamente ai Referenti informatici o al Supporto Utenza dell'Ufficio 3 di Staff le opportune verifiche;
- qualora venga ipotizzata o rilevata la presenza di virus informatici sulla propria PdL o su supporti removibili ad essa collegati, l'utente deve sospendere qualsiasi operazione in corso, spegnere il computer e contattare immediatamente il Referente Informatico o il Supporto Utenza dell'Ufficio 3 di Staff, fornendo ogni collaborazione utile per agevolare il ripristino finale della PdL;
- non è consentito scaricare o utilizzare file o programmi di incerta provenienza, tenendo presente che in alcuni casi il rischio può provenire anche da fonti pubbliche (es. Università, ecc.);
- è opportuno non dare credito a segnalazioni di virus ricevute via e-mail che non provengano dal Supporto Utenza dell'Ufficio 3 di Staff, per evitare di incorrere in falsi allarmi finalizzati a creare panico e a sovraccaricare i sistemi di posta.

6. La comunicazione interna ed esterna

L'accesso alla Rete istituzionale (LAN) permette la comunicazione di ciascuna risorsa informatica con l'insieme delle applicazioni e dei servizi che costituiscono il Sistema Informativo dell'Agenzia, nonché l'accesso ad Internet e ai servizi di posta elettronica.

L'accesso alla LAN Interna e ai relativi servizi è reso disponibile a tutti gli utenti ai quali vengono assegnate le credenziali, come precedentemente previsto (v. cap. 4 "Gestione delle credenziali di autenticazione").

A fronte di giustificata richiesta formale avanzata dal Dirigente/Responsabile della struttura di riferimento all'Ufficio 3 di Staff, può essere effettuato l'accesso dall'esterno ai servizi e alle applicazioni della LAN Istituzionale tramite collegamento in VPN, previa assegnazione delle relative credenziali a cura del Supporto Utenza dell'Ufficio 3 di Staff, che provvederà anche a fornire il manuale d'uso della VPN.

6.1. Posta elettronica

Si evidenzia che l'uso della posta elettronica è, per sua natura, estremamente delicato e quindi il linguaggio deve essere adeguato: conciso, comprensibile, dignitoso e rispettoso, nel contenuto e nei toni, e ispirato ai valori fondamentali di comportamento rappresentati nel "Codice di comportamento e di tutela della dignità e dell'etica". Inoltre, per i messaggi rivolti a soggetti esterni all'Agenzia, è essenziale essere sempre consapevoli del fatto che il mittente ultimo dei messaggi inviati risulta essere l'Amministrazione.

Per quanto riguarda l'interazione dell'utilizzo dello strumento della posta elettronica con i processi lavorativi, si sottolineano i seguenti punti:

- I temi trattati nei messaggi di posta elettronica non possono essere considerati notificati per il semplice fatto che la stessa e-mail è stata trasmessa, ma il mittente deve comunque seguirne l'iter e il suo compimento, soprattutto nel caso si tratti di adempimenti rilevanti, urgenze e scadenze.
- Il Direttore Generale dovrà essere specificato "in conoscenza" solo se realmente ed effettivamente pertinente.

- Le note, gli appunti e i documenti non possono essere considerati come sottoposti alla firma del Direttore Generale se trasmessi via e-mail.

6.1.1. Posta elettronica ordinaria

La casella di posta elettronica assegnata all'utente e contrassegnata dal seguente indirizzo (*nome.cognome*@agenziacoesione.gov.it) è uno strumento di lavoro di cui va presa visione quotidianamente (v. art. 2 del "Codice di comportamento e di tutela della dignità e dell'etica"), e gli assegnatari sono responsabili del corretto utilizzo della stessa per le finalità istituzionali. Il personale esterno avrà un indirizzo per la casella di posta del tipo: *nome.cognome*.esp@agenziacoesione.gov.it .Per un corretto uso della posta elettronica è necessario attenersi alle regole di seguito riportate:

- L'indirizzo di posta elettronica istituzionale non deve mai essere utilizzato per registrarsi ed autenticarsi su servizi web esterni all'Amministrazione (es. registrazione a siti Internet e social network), a meno che tale registrazione non sia funzionale ad esigenze professionali o per l'adesione ad iniziative/convenzioni istituzionali.
- Nei periodi di assenza prolungata dal lavoro, è buona norma impostare messaggi di risposta automatica, eventualmente contenenti le coordinate di un altro soggetto, o altre utili modalità di contatto con il proprio ufficio.
- Non scaricare allegati o aprire link presenti in e-mail sospette, ma contattare il Supporto Utenza dell'Ufficio 3 di Staff per verificare possibili casi di phishing; al riguardo è necessario fare attenzione, per esempio, ad e-mail inviate da mittenti sconosciuti ed a contenuto generalmente di natura commerciale, contenenti richieste di informazioni personali per motivi non ben specificati (ad es. scadenza, smarrimento, problemi tecnici), o aventi toni intimidatori (ad es. minaccia del blocco della carta di credito o del conto corrente in caso di mancata risposta dell'utente).
- Le comunicazioni scambiate tramite posta elettronica sono considerate di solo interesse dell'Amministrazione. Per motivi tecnici e di sicurezza, i messaggi di posta possono essere archiviati dall'Amministrazione al solo scopo di prevenire o risolvere malfunzionamenti, nonché per permetterne l'accesso eventuale alle Autorità competenti. È essenziale essere sempre consapevoli del fatto che il mittente ultimo dei messaggi inviati risulta essere l'Amministrazione. L'impiego della posta elettronica dell'Amministrazione per la partecipazione a dibattiti, forum, mailing-list, ecc. deve essere esplicitamente autorizzato dal Dirigente/Responsabile della struttura di riferimento.
- Non è consentito, per nessuna ragione, lo scambio e l'archiviazione di messaggi di posta elettronica aventi natura discriminatoria o oltraggiosa. Si rimanda inoltre a quanto previsto dal D.Lgs.196/03 in relazione ai messaggi contenenti dati personali, sensibili o giudiziari e al "Codice di comportamento e di tutela della dignità e dell'etica" dell'Agenzia per la Coesione Territoriale;
- Non è consentito spedire o inoltrare posta contenente materiale pubblicitario.

- Non è consentito diffondere "Catene di S. Antonio" o appelli/richieste non pertinenti alla propria attività lavorativa, ovvero l'inoltro reiterato di e-mail ad un numero elevato di utenti; in caso di ricezione, segnalarne il fatto via e-mail al Referente Informatico e al Supporto Utenza dell'Ufficio 3 di Staff.

- E' opportuno evitare di inviare e-mail con allegati di grandi dimensioni, se non strettamente necessario per motivi di servizio (anche comprimendo i file più grandi, ricorrendo a formati quali ad esempio *.zip, *.jpg, ecc), o e-mail che, pur veicolando allegati di dimensioni contenute, utilizzano liste di distribuzione con numerosi contatti. Si invita a porre la massima attenzione all'identità del destinatario, qualora si dovessero inviare e/o inoltrare messaggi contenenti informazioni istituzionali verso account di posta elettronica personale/free (ad esempio, gmail, tiscali, ecc.)

- I messaggi con molti destinatari, così come l'utilizzo indiscriminato dell'opzione "Rispondi a tutti", possono determinare il deterioramento delle prestazioni del Sistema di Posta. Al fine di evitare disservizi e problemi per tutti gli utenti, è quindi conveniente limitarne l'utilizzo a particolari e motivate esigenze di servizio, per le quali è raccomandato rivolgersi preventivamente al Referente Informatico e al Supporto Utenza dell'Ufficio 3 di Staff. Si ricorda inoltre che l'invio di messaggi aventi in indirizzo più destinatari può rappresentare una violazione alla vigente normativa sulla privacy.

- Non è permesso scambiare messaggi falsificando l'identità del mittente.

- Nel caso in cui si ricevano e-mail da un sito o un servizio ai quali si ritiene di non essere registrati, è opportuno evitare di cliccare su eventuali link per la cancellazione o l'"unsubscribe" dalla lista di distribuzione che, in alcuni casi, segnalando al mittente che l'indirizzo è attivo, potrebbe determinare l'inoltro di ulteriori messaggi di posta indesiderati. In caso di dubbi sul comportamento da adottare è opportuno fare riferimento al Referente Informatico o al Supporto Utenza dell'Ufficio 3 di Staff.

- Si evidenzia che, come previsto dal Garante della Privacy, qualora sia assolutamente necessario accedere per ragioni d'ufficio ad una casella di posta, in caso di assenza improvvisa e prolungata del titolare, l'interessato può delegare un "fiduciario" per la verifica del contenuto dei messaggi e l'inoltro al Dirigente di riferimento di quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Si ricorda infine che è possibile accedere ai servizi di posta elettronica dell'Amministrazione anche attraverso il sistema di web mail (Postaweb), raggiungibile tramite Internet all'indirizzo https://mail.agenziacoesione.gov.it. L'utente dovrà autenticarsi mediante le consuete credenziali di accesso. Per motivi di sicurezza, è prevista la disconnessione automatica della sessione dopo 15 minuti di inattività.

6.1.2. Posta elettronica certificata

La Posta Elettronica Certificata (PEC) è il sistema attraverso il quale è possibile inviare mail con valore legale equiparato a quello di una raccomandata con ricevuta di ritorno. In ogni caso, è fatto divieto di utilizzare le caselle PEC per motivi diversi da quelli strettamente legati all'attività lavorativa, ed in particolare di natura personale.

Le persone incaricate all'uso delle caselle di PEC – da individuarsi direttamente nel singolo utente, ove l'indirizzo PEC fosse direttamente riconducibile a questo, ovvero nel Dirigente dell'ufficio, qualora l'indirizzo PEC fosse riconducibile a tale area – sono direttamente responsabili del loro corretto utilizzo. Il Dirigente può autorizzare un dipendente dell'ufficio alla gestione della casella PEC.

I messaggi inviati tramite la casella PEC cui accede l'incaricato dovranno essere pertinenti alle specifiche mansioni lavorative attribuite e, qualora impegnativi per l'Amministrazione, rientrare nelle competenze dello stesso incaricato, come risultanti dai poteri conferiti.

La casella PEC deve essere consultata giornalmente, (v. art.. 2 del "Codice di comportamento e di tutela della dignità e dell'etica") dal personale autorizzato e munito delle credenziali di autenticazione fornite dall'Ufficio 3 di Staff. I messaggi pervenuti dovranno essere protocollati, aggiungendo, oltre alle informazioni contenute nello stesso messaggio (data di ricezione, mittente e oggetto), anche gli utenti interni cui è stata trasmessa, con relativa data di inoltro.

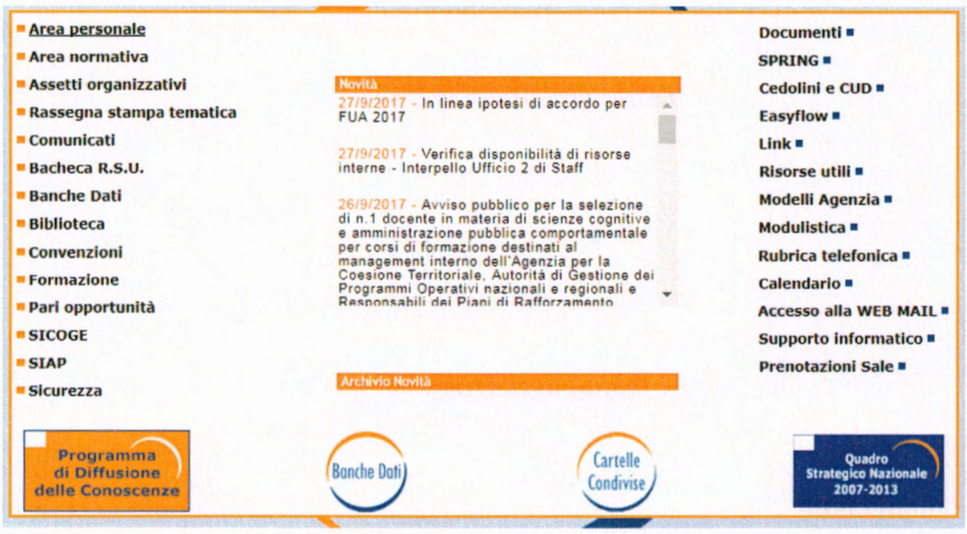
Al fine di garantire la funzionalità delle caselle PEC, sia con riferimento a PEC relative a singoli addetti, sia a quelle riconducibili a singole aree, spetterà al Dirigente gestire le situazioni di assenza dell'eventuale incaricato, così da garantire il costante e perdurante compimento delle funzioni specificate nel presente disciplinare.

Tutte le comunicazioni pervenute sulla specifica casella PEC (compresi gli eventuali documenti allegati) devono essere archiviate separatamente - al di fuori della stessa casella - a cura dell'incaricato autorizzato. In ogni caso, va garantita la conservazione dei documenti ed atti secondo le vigenti disposizioni di legge.

Resta obbligatorio porre la massima attenzione per i messaggi ricevuti nella singola casella PEC e nell'aprire gli eventuali allegati prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o Ftp non conosciuti).

6.2. Intranet

Al momento dell'accensione della PdL assegnata, l'utente sarà automaticamente indirizzato alla pagina iniziale della rete Intranet:



La Home Page della Intranet (mostrata nella figura sopra) è anche richiamabile anche attraverso il link: http://intranet.dps.tesoro.it/

La Intranet è un importante strumento istituzionale, messo a disposizione dell'utente per la conoscenza di informazioni inerenti l'organizzazione interna, per la consultazione di documenti di rilevanza istituzionale e della normativa interna; inoltre, fornisce il punto di accesso per la maggior parte degli applicativi disponibili, per gli ambienti conoscitivi, per il sistema di web mail (Postaweb), per le unità di rete condivise e per una serie di funzioni di utilità (quali rubrica telefonica, modulistica, ecc).

In particolare, attraverso la finestra delle "Novità" vengono diffuse segnalazioni, aggiornamenti e notizie rilevanti, di cui si raccomanda all'utente la consultazione quotidiana.

6.3. Internet

6.3.1. Accesso alla rete Internet

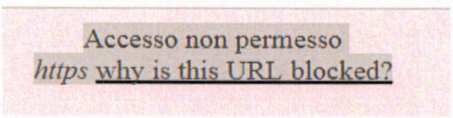
La navigazione in Internet, e l'utilizzo delle relative funzionalità, deve avvenire esclusivamente per le esigenze connesse alle attività istituzionali. Occorre quindi tener presente che qualsiasi operazione (accesso a siti WEB, scaricamento di file, partecipazione a forum, ecc.), viene effettuata a nome dell'Amministrazione, ed è pertanto fondamentale mantenere un comportamento lecito, tale da non compromettere il buon nome dell'Amministrazione stessa. Per un uso appropriato del servizio di navigazione in Internet è opportuno attenersi alle seguenti regole:

- utilizzare Internet per fini leciti, evitando l'accesso a siti non pertinenti alle mansioni assegnate e astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa o discriminatoria verso terzi;
- operare sempre utilizzando la propria identità;
- attenersi alle normative in materia di diritto di proprietà intellettuale, con riferimento al materiale fruibile su Internet;
- evitare la registrazione a siti Internet i cui contenuti non siano inerenti all'attività lavorativa;
- non partecipare, per motivi non connessi alla prestazione lavorativa, a forum, chat line, social network ecc.;
- astenersi dall'effettuare operazioni di trading on line per uso personale, dall'accedere a siti relativi a giochi e di gaming on line (scommesse) o utilizzare audio e video non inerenti l'attività professionale;

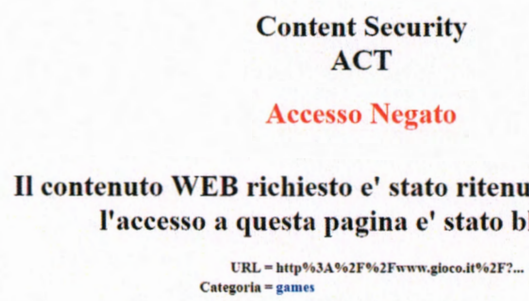
Eventuali comportamenti attuati in violazione delle disposizioni istituzionali in materia di utilizzo della posta elettronica e dell'accesso ad Internet potranno dare luogo, in relazione alla loro gravità, all'adozione di provvedimenti disciplinari, secondo la normativa vigente.

6.3.2. Analisi dei contenuti della navigazione web

Qualora, durante la navigazione in Internet, l'utente incorra in pagine che le politiche dell'Amministrazione reputino insicure, pericolose o illegali (black list), la navigazione verrà interrotta, e contestualmente verrà visualizzato uno dei messaggi di seguito riportati:



oppure



In questo caso, laddove l'utente ritenga invece che le pagine di suo interesse rientrino nella categoria della liceità, potrà avvisare via e-mail della presunta anomalia il Referente Informatico e il Supporto Utenza dell'Ufficio 3 di Staff.

La black list viene aggiornata periodicamente, in linea con le prassi adottate da altre Pubbliche Amministrazioni, a cura dell'Ufficio 3 di Staff.

6.4. Social Network istituzionali

6.4.1. Twitter

Twitter è una piattaforma gratuita che permette di condividere brevi messaggi.

Lo scopo dell'area Twitter istituzionale è quello di divulgare le attività svolte dall'Agenzia per la Coesione Territoriale, rilanciando anche i contenuti del sito Internet, e di animare l'interazione con il pubblico di questo social, facendo cronaca delle politiche di coesione.

Per poter accedere via web: https://twitter.com/agenziacoesione

La gestione e la redazione è affidata all'Ufficio 1 di Staff, che attualmente ne cura anche la parte sicurezza (password di accesso), ed è responsabile della custodia delle credenziali di accesso in modifica. Tutti gli altri utenti possono accedere in sola consultazione.

6.5. Wi-Fi

Il Wi-Fi consente a un dispositivo (computer, cellulare, palmare, tablet ecc.) di collegarsi ad una rete locale in modalità wireless (WLAN). L'Amministrazione mette a disposizione degli utenti due modalità di accesso alla rete Internet con connessione Wi-Fi, senza alcuna possibilità di ingresso sulla rete o di accesso a servizi interni, e quindi in totale sicurezza:

1. Per il personale interno ed esterno della sede di V. Sicilia, la rete denominata "WIFI-DPS". Le credenziali e le modalità per l'utilizzo vengono conferite - su richiesta del Dirigente/Responsabile della struttura di riferimento dell'utente al Dirigente dell'Ufficio 3 di Staff - dal Supporto Utenza dell'Ufficio 3 di Staff, dopo configurazione del dispositivo dell'utente (smartphone, tablet, computer portatile);

2. Per tutti gli ospiti della sede di V. Sicilia, limitatamente alle Sale Riunioni a livello -1, la rete denominata "Ospiti-DPS", che consente l'uso della rete in assenza di campo telefonico. Le credenziali (utenza e password) vengono conferite da una procedura automatica via browser, che guida l'ospite alla definizione della connessione sul proprio dispositivo portatile.

7. Condivisione dei documenti

7.1. File Sharing

È buona norma evitare la condivisione con altri utenti di file o cartelle presenti sulla propria PdL. A tale scopo, si raccomanda di utilizzare il servizio di condivisione di file e cartelle presenti sulle unità di rete condivise (file sharing).

Si precisa altresì che il servizio di file sharing deve essere utilizzato per le sole finalità di servizio, avendo cura di eliminare periodicamente i file obsoleti o inutili ed evitando l'archiviazione di dati ridondanti. Qualunque file non legato all'attività lavorativa non può essere collocato, nemmeno per brevi periodi, in queste aree dati. L'Amministrazione si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema, o acquisiti in violazione di quanto previsto dal presente documento.

7.2. Cloud ACT

I servizi informatici dell'Agenzia per la Coesione Territoriale mettono a disposizione un portale in ambiente Cloud, attraverso il quale è possibile via web salvare, condividere e scambiare documenti tra utenti interni ed esterni all'Agenzia. Relativamente alla riservatezza e l'integrità dei file caricati nel portale, è cura e responsabilità degli utenti, che ne determinano il livello di condivisione e l'utilizzo , effettuare un uso corretto della piattaforma Cloud messa a disposizione dall'Amministrazione.

Per autenticarsi al portale, il Dirigente/Responsabile della struttura di riferimento dell'utente deve inoltrare una richiesta via posta elettronica al Supporto Utenza dell'Ufficio 3 di Staff, che provvederà a creare le credenziali di accesso e a rispedirle al richiedente, insieme al manuale di utilizzo del Cloud ACT, sempre via e-mail. I dati forniti dagli utenti, utili all'accesso al servizio Cloud (nome, cognome e indirizzo e- mail), saranno gestiti in sicurezza dal Supporto Utenza dell'Ufficio 3 di Staff.

E' possibile accedere al portale selezionando la seguente Url:

https://cloud.agenziacoesione.gov.it/act

I documenti memorizzati nel portale saranno conservati finché l'utente non provvederà alla loro cancellazione; l'Amministrazione provvederà a rimuovere i file e le cartelle appartenenti all'utente solo nel caso di cancellazione dell'account utente.

8. Cessazione del rapporto di lavoro

Al termine del rapporto di lavoro con l'Amministrazione, l'utente deve mettere a disposizione della stessa ogni risorsa a lui assegnata, con riferimento sia alle attrezzature informatiche sia alle informazioni di interesse di servizio, avendo cura di eliminare i dati personali eventualmente presenti sui dispositivi di memorizzazione. In particolare, si richiama l'attenzione sulle seguenti regole:

- la casella di posta elettronica individuale sarà mantenuta attiva per il tempo strettamente necessario a gestire il passaggio di consegne e concludere eventuali contatti aperti;
- le informazioni di interesse di servizio presenti sulla PdL e sulle unità di rete condivise non dovranno essere cancellate dall'utente senza esplicita autorizzazione del Dirigente responsabile;
- le informazioni non attinenti all'attività di servizio, eventualmente ancora memorizzate sulle postazioni di lavoro riconsegnate o sulle unità di rete condivise, verranno cancellate a cura dell'Amministrazione.

9. Considerazioni finali

Considerato che in caso di violazioni contrattuali e giuridiche, sia l'Amministrazione sia l'utente sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Amministrazione si riserva di verificare, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio Sistema Informativo. Si ribadisce che i dati memorizzati a tal fine attraverso file di log non saranno utilizzati in alcun modo per il controllo a distanza dei lavoratori.

Il mancato rispetto di quanto stabilito nel presente documento può comportare conseguenze disciplinari.

Quanto non sia contemplato in questo Disciplinare non è consentito, se non espressamente autorizzato dal Dirigente/Responsabile della struttura di riferimento e dal Dirigente dell'Ufficio 3 di Staff. La messa in atto di comportamenti difformi avviene sotto la diretta responsabilità dell'utente.

Il presente disciplinare sarà sottoposto ad una revisione periodica, al fine di garantirne il costante aggiornamento in relazione all'evoluzione della normativa e allo sviluppo degli strumenti tecnologici del Sistema Informativo.

APPENDICE: Glossario

Definizione o Acronimo	*Descrizione*
Amministrazione	Agenzia per la Coesione Territoriale
Attacco informatico	Tentativo di accesso non autorizzato ad un sistema informatico al fine di compromettere la disponibilità e le funzionalità del sistema stesso o anche la riservatezza, l'integrità o la disponibilità dei dati/informazioni in esso contenuti
Cloud	Insieme di risorse informatiche, come trasmissione, condivisione o archiviazione di dati, caratterizzato dalla immediata fruibilità attraverso Internet
Dominio	Rete di computer che vengono amministrati come un'unità, con regole e procedure comuni
Dotazione Informatica o Strumento Informatico	Dispositivo hardware o software reso disponibile dall'Amministrazione. Ad esempio: computer portatile o fisso, tablet, smartphone e telefono cellulare, badge, token, smart card, posta elettronica, accesso ad Internet, connessione VPN, stampanti, dispositivi di archiviazione di massa (memorie flash, drive esterni, ecc.)
Ftp	File transfer protocol - Protocollo per il trasferimento di file
PdL (Postazione di Lavoro)	Personal Computer configurato almeno con mouse, tastiera, monitor, scheda di rete LAN e porte USB o Personal Computer portatile (con scheda Wi-Fi), dotati di sistema operativo e di software relativo alla produttività individuale
Phishing	Truffa consistente nel tentativo di indurre con l'inganno a fornire informazioni personali sensibili o riservate attraverso l'uso di strumenti informatici (siti web fasulli, messaggi di posta elettronica con link o allegati dannosi, ecc.)
Referenti Informatici	Gruppo di assistenza tecnica, costituito da personale dell'Ufficio 3 di Staff, che opera a supporto delle esigenze espresse dall'utenza in relazione all'utilizzo degli strumenti informatici.
Screen Saver (Salvaschermo)	Programma che provoca il blocco e l'oscuramento dello schermo, o la comparsa di un'animazione sullo stesso dopo un tempo prestabilito di inattività della tastiera e del mouse, impostabile attraverso le funzioni del sistema operativo, che consente normalmente la ripresa delle attività solo con una nuova immissione delle credenziali utente.
Smart Card	Dispositivo hardware della dimensione di una carta di credito con potenzialità di elaborazione, memorizzazione dati o interfaccia input/output
Social Network	Servizio Internet, fruibile mediante browser o applicazioni mobili, per la gestione dei rapporti sociali, che consente la condivisione di testi ed immagini.
Token	Dispositivo fisico utilizzato per l'autenticazione a servizi, dispositivi o sistemi
Unità di rete condivisa (File Sharing)	Spazio di archiviazione su memorie centralizzate gestito e protetto dall'Amministrazione, e fornito agli utenti in modalità condivisa
Utente	Utilizzatore delle risorse fornite dall'Amministrazione con tecnologie informatiche
USB (Universal Serial Bus)	Interfaccia standard che fornisce un unico protocollo di comunicazione per la connessione tra computer e periferiche elettroniche
Virus	Tipologia di software dannoso in grado di interferire con il corretto funzionamento di altri programmi, di replicarsi e di diffondersi attraverso le reti di comunicazione, provocando, in taluni casi, il degrado o l'indisponibilità dei sistemi infettati
VPN	(Virtual Private Network). Rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la rete Internet