SERVIZIO 01-DIREZIONE GENERALE

Decreto numero 92 – Registro Generale del 19-02-2018

N. 11 Settoriale

COPIA

OGGETTO:	**APPROVAZIONE DEL CODICE INTERNO PER L'USO DELLE RISORSE E STRUMENTAZIONE INFORMATICA**

IL RESPONSABILE DEL SERVIZIO

VISTI:

- il 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 che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in vigore del 24 maggio 2016, e applicabile a partire dal 25 maggio 2018;
- la L. 25 ottobre 2017, n. 63 "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017*" che all'art. 13 demanda al Governo il compito di adottare i decreti legislativi per adeguare entro sei mesi il quadro normativo nazionale al Regolamento UE 2016/679 (GDPR) con successive modifiche al d.lgs. 163/2003;
- il vigente D.lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personale**";**
- la Legge 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
- il Decreto Legislativo 7 marzo 2005, n. 82 "*Codice dell'amministrazione digitale – CAD*";
- il Decreto Legislativo 30 dicembre 2010, n. 235 "*Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69*";

VISTA la legge regionale 5 dicembre 2008, n.31 "Testo unico delle leggi regionali in materia di agricoltura, foreste, pesca e sviluppo rurale", con particolare riferimento al Titolo V "Ente Regionale per i Servizi all'Agricoltura e alle Foreste (ERSAF);

VISTO, altresì:

- l'art. 65 della sopracitata legge che, tra l'altro, stabilisce:

al comma 14 che *<<il Direttore dispone della corretta ed efficace esecuzione degli atti finalizzati al raggiungimento degli obiettivi (...) ed esercita le altre funzioni attribuitegli dallo statuto e dai regolamenti>>*;

RICHIAMATI:

- lo Statuto di ERSAF, approvato con Deliberazione del Consiglio di Amministrazione n. II/0227 del 25/01/2011, e ss.mm.ii., che all'articolo 16, comma 8, dispone che il Direttore è preposto alla gestione del

personale e al funzionamento dell'Ente;
- la Deliberazione del Consiglio di Amministrazione n. III/140 del 30/04/2015 ad oggetto "Conferimento incarico Direttore ERSAF"

CONSIDERATO che la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i sistemi di elaborazione, espone l'Ente a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

RITENUTO che le attrezzature informatiche, i relativi programmi e/o applicazioni, i dati e documenti affidati in uso agli operatori sono strumenti di lavoro, di cui l'Ente può disporre unilateralmente, essendo titolare di qualsiasi diritto ad essi correlato.

VISTA la proposta di "Codice Interno per l'uso delle risorse e strumentazione informatica dell'ERSAF", allegato A, predisposta dalla Struttura dirigenziale competente per i Servizi infotelematici (UO Programmazione, Servizi Generali e Sviluppo Territoriale Lombardia Ovest) ed il relativo allegato che contiene le specifiche del servizio di backup delle postazioni di lavoro (PdL) messe in atto nell'ambito del progetto ARCA DTM relativo alla fornitura di hardware e software in uso nell'ente, tutti parte integrante e sostanziale del presente atto;

PRESO ATTO CHE Su raccomandazione espressa dall'Autorità Garante per la Protezione dei Dati personali (deliberazione n.13 del 1 marzo 2007), tutti i punti indicati nel presente codice sono stati sottoposti alle Organizzazioni Sindacali con nota di trasmissione prot. ERSAF n. 2017.0016434 del 18.12.2017 e al Comitato Unico di Garanzia per le pari opportunità, la valorizzazione del benessere di chi lavora e contro le discriminazioni che lo ha esaminato in data 11.01.2018;

DECRETA

Recepite le premesse che formano parte integrante del presente provvedimento,

1. di approvare il "Codice Interno per l'uso delle risorse e strumentazione informatica" Allegato A, parte integrante e sostanziale del presente atto;
2. di pubblicare:
   - sul Portale Internet e sulla rete Intranet di ERSAF il presente atto con il relativo Allegato.

Lì, 19-02-2018

IL RESPONSABILE DEL SERVIZIO
F.to ORNAGHI MASSIMO

Copia di documento originale firmato digitalmente ai sensi del D.lgs. 82/2005 e norme collegate.

ERSAF
ENTE REGIONALE PER I SERVIZI ALL'AGRICOLTURA E ALLE FORESTE

RegioneLombardia

CODICE INTERNO PER L'USO DELLE RISORSE E STRUMENTAZIONE INFORMATICA

Premessa

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete tramite i sistemi di elaborazione, espone l'Ente a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

I sistemi informatici sono soggetti a vulnerabilità e attacchi volti all'accesso ai dati in esso contenuti oppure a minarne la funzionalità o disponibilità di servizio. Spesso dal funzionamento o meno del sistema informatico dipende anche la sicurezza dei dati in esso contenuti.

L'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

Le attrezzature informatiche, i relativi programmi e/o applicazioni, i dati e documenti affidati in uso agli operatori sono strumenti di lavoro, di cui l'Ente può disporre unilateralmente, essendo titolare di qualsiasi diritto ad essi correlato. Tutto quanto messo a disposizione, ricevuto, rilasciato e comunque memorizzato per attività lavorative è e rimane di proprietà dell'Ente.

1. Scopo e campo di applicazione

Alla luce di quanto premesso, ERSAF adotta il presente Codice interno al fine di:

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- informare gli operatori di quali sono le misure di tipo organizzativo e tecnologico adottate dall'Ente per la sicurezza dei dati;
- illustrare quali sono le modalità di utilizzo consapevole e diligente delle risorse messe a disposizione;
- comunicare agli operatori le finalità e le modalità dei controlli che l'Ente potrebbe effettuare sulle risorse messe a disposizione per lo svolgimento delle attività istituzionali.

Questo Codice non si riferisce solamente all'utilizzo di internet o della rete locale, ma si riferisce a tutto l'insieme delle risorse informatiche, di calcolo, di comunicazione, elettroniche, audiovisive e a qualsiasi altra tipologia di risorsa infotelematica presente nell'Ente.

Tutti i contratti che verranno conclusi tra l'Ente e soggetti terzi a cui viene permesso l'accesso ai dati, ai programmi informatici o ad altri mezzi dell'Ente, dovranno riportare una clausola che impegni le parti a rispettare il presente Codice; ciò indipendentemente dalla nomina a incaricato o a responsabile del trattamento dati ai sensi della normativa vigente in tema di protezione dei dati personali.

Per i contratti conclusi dall'Ente con soggetti esterni si dovrà prevedere in essi l'atto bilaterale di nomina a Responsabile del trattamento dei dati ai sensi del Regolamento UE 2016/679 (GDPR) indicando i soggetti competenti (per Ersaf il Direttore generale).

2. Soggetti destinatari del presente documento

Il presente documento è indirizzato a tutto il personale dipendente di ERSAF, compreso il personale dirigenziale, a tutti coloro che collaborano con ERSAF nel momento in cui usano le attrezzature informatiche dell'ente, ed a tutti coloro i quali, pur in assenza di un rapporto di lavoro subordinato con l'Ente, collaborano con esso a qualunque titolo o grado. I soggetti sopra indicati sono tutti egualmente obbligati al rispetto degli obblighi derivanti dall'applicazione del presente codice.

3. Definizioni

TITOLARE DEL TRATTAMENTO DEI DATI: è la figura individuata dall'art. 28 del D.Lgs. 196/2003. Vigila sulla puntuale osservanza di tutte le disposizioni in materia di trattamento dei dati. Designa tutte le altre figure coinvolte nel trattamento informatico dei dati.

RESPONSABILE DEL TRATTAMENTO: è la figura prevista dall'art. 29 del D.Lgs. 196/2003 ed è nominata dal Titolare. Garantisce il pieno rispetto delle vigenti disposizioni in materia di trattamento (anche informatico) dei dati; i compiti affidati al responsabile sono analiticamente specificati per iscritto dal Titolare al momento della nomina.

RESPONSABILE DELLA STRUTTURA COMPETENTE PER I SERVIZI INFOTELEMATICI: è la figura, designata dal Titolare, che gestisce e coordina le attività di installazione, configurazione e aggiornamento dei sistemi e degli archivi informatici. Il ruolo del Responsabile è solo quello di coordinatore dell'applicazione della normativa sulla riservatezza dei dati in ambito informatico, ferme restando le responsabilità in merito all'adozione degli atti (nomina incaricati, rilevazione banche dati, istruzione agli incaricati, ecc).

AMMINISTRATORI DI SISTEMA: sono le figure, designate dal Titolare, che provvedono operativamente alla gestione e manutenzione del sistema informatico sulla base delle misure organizzative fissate dal responsabile della Struttura competente per i Servizi infotelematici in linea con quanto indicato dal Garante della Privacy nel suo provvedimento del 27 Novembre 2008 e aggiornamenti successivi.

INCARICATO DEL TRATTAMENTO: è la figura prevista dall'art. 30 del D.Lgs. 196/2003 ed è nominata dal Responsabile o dal Titolare del trattamento; tratta i dati sia in forma cartacea sia attraverso strumenti informatici; opera sotto la diretta autorità del Responsabile del trattamento, attenendosi alle istruzioni impartite.

CUSTODE DELLE PASSWORD: ove i sistemi informatici o le banche dati, non consentano una gestione automatizzata delle password e sia necessario tenere traccia di una password per iscritto, viene nominato un custode della password che provvede a conservarla. Possono essere nominati custodi diversi per password differenti, a seconda della necessità e del contesto organizzativo.

TRACCIAMENTO: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso senza ledere i diritti del dipendente stabiliti dalla normativa in materia di privacy.

RILEVAZIONE: complesso di operazioni di analisi e verifica dei tracciamenti effettuati dai dispositivi e di qualsiasi altra informazione di carattere professionale inerente il funzionamento e l'utilizzo delle risorse informatiche, svolte da Amministratori di Sistema a fronte di comprovate necessità definite nei capitoli seguenti del presente disciplinare.

4. Funzionamento delle risorse informatiche

Le risorse informatiche tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia delle risorse stesse.

Il tracciamento di tali eventi non è generalmente oggetto di rilevazione da parte dell'ufficio Sistemi Infotelematici. Il personale tecnico incaricato dall'Ente potrà svolgere rilevazioni di dati su una risorsa specifica per necessità manutentive o di gestione della sicurezza, nel rispetto della dignità e della libertà dei lavoratori, con le modalità indicate di seguito nel documento.

5. Dati trattati attraverso le risorse informatiche concesse in dotazione

Le risorse informatiche sono messe a disposizione dall'Ente agli utenti per finalità legate alle attività istituzionali dell'Ente stesso, pertanto l'utilizzo degli strumenti in dotazione e il trattamento è di prevalente carattere professionale.

È consentito l'utilizzo per finalità personali della postazione di lavoro a condizione che:

- Venga effettuato al di fuori dell'orario di lavoro o durante le pause;
- Non sia contrario alle regole di condotta indicate nei paragrafi successivi e non possa in alcun modo ledere l'immagine dell'Ente;
- Non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- Non comporti alcuna violazione di norme giuridiche;
- Sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente. A titolo esemplificativo si precisa che nel caso in cui ricadano su Ersaf le conseguenze di uso improprio della strumentazione informatica da parte degli utenti, l'ente adotterà tutte le misure necessarie per poter risalire al soggetto che sarà ritenuto direttamente responsabile.

È importante precisare che è consentito l'utilizzo personale esclusivamente della postazione di lavoro, compresa la navigazione Internet in siti legali; non è in alcun modo consentito trattare dati di cui l'Ente è Titolare del Trattamento se non per attività di carattere professionale.

È ammessa la custodia di dati personali sulla postazione di lavoro a condizione che:

- Siano riposti in cartelle di cui sia esplicitamente indicata la privatezza del dato (es. cartelle con dicitura “personale”);
- Siano esplicitamente differenziabili dai dati trattati per attività professionali;
- Vengano rimossi prima del rilascio della postazione di lavoro.

Alla riconsegna delle attrezzature la rimozione dei dati personali è a carico degli utenti. L’Ente, a seguito della riconsegna, potrà liberamente disporre dei dati ivi presenti. Qualora le risorse informatiche riconsegnate dovessero contenere dati personali relativi agli utilizzatori, il trattamento di tali dati verrà effettuato secondo i principi di pertinenza e non eccedenza previsti dalla normativa sulla protezione dei dati personali. Eventuali dati personali ancora residenti al momento della riconsegna della postazione verranno rimossi indiscriminatamente.

Tutti i dati e i documenti trattati durante lo svolgimento delle attività professionali svolte in nome e per conto dell’Ente sono di proprietà esclusiva dell’Ente stesso, pertanto devono essere lasciati a completa disposizione dell’Ente al momento della riconsegna delle attrezzature.

6. Utilizzo delle Postazioni di lavoro

La postazione di lavoro affidata al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente l’attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l’utilizzo improprio dello stesso.

Non è consentito installare programmi provenienti dall’esterno salvo preventiva autorizzazione dei tecnici debitamente incaricati, onde evitare il grave pericolo di introdurre minacce informatiche nonché di alterare la stabilità delle applicazioni dell’elaboratore.

Non è consentito l’uso di programmi diversi da quelli messi a disposizione o autorizzati dall’Ente stesso, in quanto l’inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l’Ente a gravi responsabilità civili e penali in caso di violazione della normativa sulla tutela del diritto d’autore, che impone la presenza nel sistema di software provvisto di regolare licenza d’uso.

Le attrezzature vengono consegnate all’utente con una configurazione coerente con le misure organizzative e di sicurezza impostate dall’Ente stesso: non è consentito all’utente di modificare le caratteristiche impostate, salvo preventiva ed esplicita autorizzazione.

Non è consentito l’utilizzo sul PC di nessun dispositivo di memorizzazione, comunicazione o altro (ad es. masterizzatori, modem …) se non con l’esplicita autorizzazione del Responsabile della Struttura competente per i Servizi Infotelematici.

Il PC deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall’ufficio, salvo specifica disposizione dei tecnici incaricati della manutenzione delle postazioni di lavoro e/o a seguito di pianificazione dello spegnimento automatico. In ogni caso, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l’uso indebito, l’utente che si allontana dalla postazione deve bloccarne l’uso.

È comunque possibile, tramite la combinazione dei tasti *CTRL+ALT+CANC* oppure tramite il blocco automatico con password, bloccare le postazioni di lavoro in caso di inattività; attivando quest'ultima funzionalità automatica si può impostare un intervallo di inattività oltre il quale entra in funzione il blocco della postazione.

Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico anche se presenti nel sistema operativo installato.

Non sono permesse, le seguenti attività:

- caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'Ente documenti, informazioni, immagini, filmati ecc. in generale, ed in particolare:
    - a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
    - illeciti in base alla normativa sul diritto d'autore;
    - pregiudizievoli per le risorse dell'Ente e per l'integrità e la conservazione dei dati dell'Ente stesso;
    - pregiudizievoli per l'immagine e il buon nome dell'Ente anche all'esterno dell'Ente stesso;
- accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate;
- tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente si trovi a ricevere anche contro il suo volere tali materiali, è tenuto a informare il personale dell'ufficio Sistemi Infotelematici e attenersi alle istruzioni impartite circa il trattamento di tali materiali;
- utilizzare le risorse dell'Ente con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure od altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, a meno che ERSAF non ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, ecc. messi a disposizione dall'Ente in violazione delle leggi sulla proprietà intellettuale, delle regole di buona tecnica applicabili e delle prescrizioni emanate dall'Ente;
- caricare o trasmettere, con volontà, archivi o programmi contenenti minacce informatiche o dati alterati;
- manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;
- inviare messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a ciò che abitualmente viene definito "*catena di S. Antonio*";
- utilizzare le risorse dell'Ente in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla legge e/o da regolamenti interni.

Poiché alcune attività sopra elencate possono avere conseguenze di natura penale, esse originano in capo al trasgressore tutte le responsabilità previste dalla legge.

Nonostante la presenza di programmi antivirus, è ritenuto statisticamente probabile che l'utilizzo di applicazioni di comunicazione (internet, posta elettronica, ecc.) e di supporti rimovibili comporti la trasmissione di virus informatici o di programmi e archivi in grado di alterare, distruggere o monitorare l'attività e i contenuti dei personal computer. La postazione viene fornita provvista di sistemi antimalware: l'utente deve verificare l'effettivo aggiornamento di tali sistemi. La verifica viene fatta controllando che l'icona relativa all'antivirus non riporti messaggi di anomalia, visivamente rappresentati da un punto esclamativo giallo posizionato sull'icona.

In caso di anomalie dell'hardware e del software affidatogli, l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso ed informare immediatamente il Servizio di assistenza della società fornitrice e il personale dell'ufficio Sistemi Infotelematici per le incombenze di competenza.

7. Utilizzo di dispositivi portatili

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dall'Ente e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Danni arrecati alle attrezzature ed ai PC o la loro perdita dovuti ad incauta custodia (se accertati) saranno a carico dell'utente utilizzatore.

Il dispositivo non deve essere lasciato incustodito in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, il dispositivo non deve essere lasciato in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque zone non custodite.

Gli utenti di attrezzature portatili si impegnano, dovunque dovessero trovarsi, a mettere in sicurezza gli strumenti in dotazione e i dati ivi contenuti.

Ai dispositivi portatili si applicano le regole di utilizzo previste per le postazioni di lavoro "fisse" e connesse alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna.

Qualora il PC portatile non sia connesso alla rete aziendale, e quindi non soggetto alla procedura automatizzata di backup delle risorse locali (come descritto nell'Allegato A) è competenza dell'utente l'effettuazione del backup dei dati residenti sulla postazione di lavoro: per tale attività può richiedere il supporto dei tecnici incaricati dall'ufficio Sistemi Infotelematici al fine di garantire la disponibilità dei dati.

Il contatto unico dell'utente è il Service Desk, che costituisce il punto di raccolta per la segnalazione di problemi informatici, risoluzione dei problemi e/o indirizzamento verso le strutture competenti.

È attivo il **canale** di contatto telefonico:

- n. 20000 (da interno) – Dopo il messaggio di accoglienza, selezione tasto 1
- n. 02 6765 0000 (da esterno) – Dopo il messaggio di accoglienza, selezione tasto 1

Orario di servizio: da Lunedì a Sabato dalle 06:00 alle 21:00

Per le attrezzature che non rientrano nel contratto con la Società fornitrice (TIM-BVtech) informare il referente interno via mail: assistenza@ersaf.lombardia.it che indicherà se è opportuno procedere con la segnalazione al contact center 20000 o se intraprendere un'azione alternativa.

8. Utilizzo dei supporti esterni

Tutti i supporti esterni (cassette, secure drive, cd, dvd, chiavi e dischi esterni USB, ecc…) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trattato da soggetti non incaricati.

I supporti contenenti dati personali, ancor più se sensibili e/o giudiziari, devono essere conservati con la massima attenzione da parte dell'utente che li utilizza: ogni eventuale conseguenza derivante dall'utilizzo inadeguato di detti supporti comporta una diretta responsabilità da parte dell'utilizzatore.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antimalware in dotazione. L'utente può richiedere il supporto dei tecnici incaricati dall'ufficio Sistemi Infotelematici nel caso in cui vengano rilevate minacce informatiche e non sia in grado di attuare autonomamente le dovute contromisure di sicurezza.

9. Utilizzo della rete LAN e delle risorse condivise

Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti che operano con postazioni fisse collegate alla LAN aziendale effettuano su cartelle di rete il salvataggio di tutti i file di lavoro; è possibile salvare i documenti anche su specifiche cartelle residenti sulla postazione, appositamente realizzate e sottoposte a backup periodico. L'elenco di tali cartelle "locali" è reso disponibile dalla Struttura competente per i Servizi Infotelematici. Tutte le altre cartelle residenti sulla postazione non sono sottoposte a procedure di backup e sono quindi inadatte alla custodia di dati e documenti informatici: non è pertanto permesso salvarvi informazioni di carattere professionale, al fine di prevenire il rischio di perdita dei dati.

È consentito conservare documenti di natura professionale sui dispositivi portatili dati in dotazione, con la consapevolezza che non sono sottoposti a procedure di backup (ad esclusione delle cartelle specificamente indicate dal personale della Struttura competente per i Servizi Infotelematici) e che pertanto la messa in sicurezza di tali dati è demandata agli utenti che, avendo ricevuto direttive dal personale della Struttura competente per i Servizi Infotelematici, hanno ricevuto tali attrezzature in dotazione.

Le cartelle/unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

Sulle cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup.

Le credenziali di accesso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con credenziali di altri utenti.

L'ufficio Personale ed ogni altra Struttura interessata dovrà comunicare alla Struttura competente per i Servizi Infotelematici ogni variazione di carattere organizzativo relativa al personale dell'Ente, al fine di consentire ai tecnici incaricati la creazione/modifica/cancellazione dei permessi di accesso alle risorse informatiche, affinché siano coerenti con le mansioni affidate al personale e il relativo trattamento dei dati. Allo stesso modo, il Responsabile dell'ufficio Sistemi Infotelematici coordinerà la consegna e il ritiro delle risorse informatiche.

Le cartelle su server sono organizzate nella maniera seguente:

- una cartella personale per ogni soggetto;
- cartelle condivise da gruppi di lavoro il cui accesso è abilitato esclusivamente ai soggetti che vi operano;
- una cartella condivisa da tutti gli uffici per consentire l'interscambio di documenti.

Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare le cartelle di scambio create a tale scopo. **Le cartelle di scambio devono essere tenute in ordine, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati a persone non espressamente incaricate.**

I Responsabili del Trattamento dovranno coordinare la periodica (almeno ogni 6 mesi) pulizia degli archivi attuando:

- la cancellazione dei file obsoleti ed inutili nelle cartelle di competenza;
- l'eliminazione delle archiviazioni ridondanti, che dovranno comunque essere evitate;
- la verifica delle cartelle in coerenza con il trattamento dei dati da parte degli uffici e dei gruppi di lavoro;
- la verifica ed eventualmente la variazione, avvalendosi dei tecnici informatici incaricati, delle "permissions" di accesso a risorse condivise affinché siano coerenti con le nomine di incarico del trattamento dati e l'operatività degli utenti.

I tecnici informatici incaricati, nell'espletamento delle mansioni attribuite loro dal Responsabile della struttura competente per i Servizi Infotelematici, possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno pericolosi per la sicurezza, sia sui PC degli incaricati sia sui server. Potranno inoltre ricorrere alla cancellazione di alcune tipologie di file al fine di liberare spazio disco sui server: tale operazione di carattere manutentivo verrà comunicata preventivamente agli utenti, che potranno segnalare eventuali eccezioni all'operazione di pulizia a fronte di motivazioni di carattere esclusivamente lavorativo.

Il Responsabile dell'ufficio Sistemi Infotelematici potrà consentire deroghe a quanto previsto dal precedente paragrafo solo dopo attenta valutazione.

È vietato il collegamento alla rete aziendale di personal computer portatili o di attrezzature informatiche non di proprietà aziendale. Il Responsabile dell'ufficio Sistemi Infotelematici

potrà consentire deroghe a quanto previsto dal precedente paragrafo solo dopo attenta valutazione.

Per quanto riguarda l'utilizzo di stampanti condivise, gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti comuni.

10. Acquisizione software

Sulle postazioni è consentita l'installazione esclusiva delle seguenti categorie di software:

- software commerciale dotato di licenza d'uso (es. pacchetti di Office Automation)
- software gestionale specificatamente realizzato da aziende specializzate nel settore della P.A. (es. applicativi in uso ai vari servizi)
- software realizzato specificatamente dagli organi centrali della Pubblica Amministrazione o Enti nazionali (es. INPS, Ministeri…)
- software gratuito (freeware) e shareware prelevato dai siti internet, esclusivamente ed espressamente installato dal personale dell'ufficio Sistemi Infotelematici
- qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative e istituzionali.

L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione con la Struttura competente per i Servizi Infotelematici, al fine di garantire la stabilità dei sistemi e la compatibilità del software con gli stessi.

11. Servizi con impatto sui sistemi informatici

L'acquisizione di materiale hardware o di qualsiasi dispositivo che interagisca con la rete e/o la strumentazione informatica dell'Ente o possa avere un impatto con essi, qualora non venga eseguita direttamente dalla Struttura competente per i Servizi Infotelematici, deve essere concordata preventivamente con essa, onde evitare malfunzionamenti, cadute prestazionali o altri problemi alla sicurezza e all'immagine dell'Ente stesso.

Qualora nell'esercizio di una funzione amministrativa sia prevista la fornitura di software accessorio alla gestione/erogazione di un servizio, l'ufficio competente per il sopracitato servizio provvede a consultare la Struttura competente per i Sistemi Infotelematici nelle fasi preliminari del processo di acquisizione, per la corretta definizione delle caratteristiche del software, affinché lo stesso risulti:

- compatibile con il sistema informativo dell'Ente,
- conforme alle misure di sicurezza adottate dall'Ente con particolare riguardo alla sicurezza degli accessi
- certificato per l'installazione sulle macchine in dotazione all'ente (server e pc)

- installato correttamente

In caso di mancata consultazione preventiva dell'ufficio Sistemi Infotelematici non verrà effettuata alcuna installazione.

Qualora venga affidata all'esterno la gestione di dati di cui ERSAF è titolare per l'erogazione di servizi, l'ufficio competente deve concordare preventivamente con la Struttura competente per i Servizi Infotelematici le modalità e i formati con cui questi dati devono essere comunicati sia in ingresso che in uscita, nonché le condizioni di consegna dei dati al termine del rapporto di collaborazione.

12. Gestione delle password e degli accessi

L'utente deve utilizzare sempre una password ogni qualvolta sia richiesto, avendo cura che nessuno ne venga a conoscenza.

Le credenziali di accesso alla rete e dello screensaver sono previste e vengono attribuite dai tecnici incaricati all'utente per il primo accesso. Dopo il primo accesso il sistema chiederà all'utente di modificare la password, la quale sarà conosciuta solo dall'utente stesso. Qualora si renda necessario (per manutenzione, aggiornamenti, assenza prolungata imprevista che renda indisponibili risorse gestite dall'utente) che il personale tecnico incaricato debba accedere al sistema con le credenziali dell'utente, la password di accesso dell'utente stesso verrà modificata. Al successivo accesso da parte dell'utente il personale tecnico incaricato gli rilascerà una password di cortesia che verrà immediatamente modificata dall'utente stesso.

L'accesso agli applicativi può a sua volta essere regolato da un'ulteriore password: le modalità di gestione e di scadenza di dette password sono specifiche per ogni programma. All'utente sarà fornito un profilo personale e verranno attivate procedure per garantire all'utente stesso la conoscenza esclusiva della propria password. Nel caso il sistema non lo consenta o sia necessario l'intervento di personale tecnico incaricato per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi.

La combinazione dell'accesso alla rete e agli applicativi garantirà il rispetto delle regole minime di sicurezza indicate nella normativa vigente in tema di protezione dei dati personali.

Le password di accesso alla rete ed agli applicativi, salvo impossibilità dovute all'obsolescenza del software, devono essere modificate almeno ogni 3 mesi e devono essere composte da almeno una minuscola, una maiuscola e un numero o carattere speciale (ricordando che maiuscole e minuscole sono interpretate diversamente dal sistema); devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.

Nel caso in cui si sospetti che una password abbia perso la segretezza, l'utente provvederà ove possibile a modificarla personalmente oppure con il supporto dei tecnici incaricati.

Non è consentito utilizzare il profilo personale di altri soggetti per accedere ai dati personali. Qualora l'utente venga a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia al personale dell'ufficio Servizi Infotelematici.

Nel caso di inserimento di password errata, si rimanda alle specifiche del software al quale si sta cercando di accedere, descritte nel manuale utente. L'assistenza ICT deve essere sempre il punto di riferimento in caso di richieste di abilitazioni.

L'utente è tenuto ad assicurare la segretezza delle password utilizzate per attività lavorative, al fine di garantire la sicurezza dei dati e dei servizi utilizzati.

Come indicato al punto 7 dell'Allegato B del Codice della Privacy "Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica".

13. Attività di backup

Sono oggetto di attività di salvataggio centralizzato:

- i file salvati sulle cartelle/unità di rete messe a disposizione dalla Struttura competente per i Servizi Infotelematici;
- le banche dati di applicativi ed i relativi file di sistema;
- le cartelle presenti sulle postazioni di lavoro specificamente identificate e comunicate agli utenti.

Le modalità di backup dei server e delle cartelle note dei client, sono descritte nel contratto quadro stipulato da ARCA e l'aggiudicatario della gara da loro effettuata, al quale ERSAF aderisce (Vedi ALLEGATO).

Le caselle di posta elettronica sono sottoposte a backup as a service, secondo il quale i messaggi vengono mantenuti in base a quanto previsto dal relativo contratto.

I dati che risiedono sulle postazioni non sono soggetti a operazioni di backup centralizzato, ad esclusione delle cartelle specificamente identificate e comunicate agli utenti.

Per quanto riguarda eventuali archivi informatici localizzati sulle postazioni di lavoro, gli utenti devono concordare, sotto loro responsabilità, l'attività di backup di risorse non incluse nell'elenco standard previsto nell'accordo quadro, insieme al personale della Struttura competente per i Servizi Infotelematici.

14. Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono attivi presso l'Ente strumenti di assistenza remota che consentono ai tecnici informatici incaricati di connettersi alle postazioni degli utenti per fornire supporto in tempo reale e assistere gli utenti nella risoluzione di problematiche di carattere informatico.

Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dei tecnici: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.

Per quanto riguarda gli interventi di assistenza remota sulle postazioni da parte di tecnici di aziende esterne, detti interventi dovranno comunque essere preventivamente concordati con l'ufficio Servizi Infotelematici e comunque comunicati al servizio stesso.

15. Posta elettronica

La casella di posta elettronica, assegnata dall'Ente all'utente, è uno strumento esclusivo di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Le caselle di posta assegnate possono essere utilizzate solo per finalità di carattere lavorativo, pertanto si assume che le informazioni veicolate tramite tale strumento non siano di carattere personale.

Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta ufficiale dell'Ente, tramite caselle di posta elettronica certificata registrate dall'Ente stesso, o tramite caselle definite ad hoc in accordo con l'ente per le diverse esigenze di progetto, anche se non registrate sul dominio Ersaf.

È consentita l'iscrizione a mailing list e servizi di carattere istituzionale che richiedano l'indirizzo di posta elettronica. In tutti gli altri casi, è fatto divieto di utilizzare le caselle di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione da parte del Responsabile dell'ufficio Sistemi Infotelematici per esigenze di lavoro.

È inoltre da evitare, ove possibile, l'invio di messaggi con allegati di grandi dimensioni al fine di evitare eventuali sovraccarichi al sistema informatico e nuocere all'efficacia della comunicazione.

La casella di posta deve essere tenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Nel caso di **trasmissione di file all'interno dell'Ente** attraverso la posta elettronica, è necessario prestare attenzione alla dimensione degli allegati, per tale motivo **è preferibile l'uso delle cartelle di rete create a tale scopo.**

È vietato inviare mail con allegati contenenti file eseguibili (estensione .exe, .bat, ecc.).

È vietato aderire a catene telematiche (o di "*S. Antonio*") che richiedono la divulgazione e circolazione di messaggi di posta di carattere non lavorativo. Se si dovessero ricevere messaggi di tale tipo, si dovrà cancellare il messaggio ricevuto senza divulgarlo in alcun modo. Non si dovranno in alcun caso attivare gli allegati di tali messaggi.

Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, ecc) di cui non è certa la provenienza, l'utente è tenuto a segnalarli immediatamente al personale dell'ufficio Servizi Infotelematici prima di effettuare qualsiasi azione.

Al fine di garantire la continuità di servizio, sono previste 2 differenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

1) ASSENZA PROGRAMMATA: attivazione da parte dell'utente di un risponditore automatico che segnali la temporanea indisponibilità all'accesso alla casella di posta, indicando eventualmente un indirizzo di posta alternativo a cui inviare il messaggio in caso di necessità di carattere professionale;
2) ASSENZA NON PROGRAMMATA: l'utente è comunque tenuto, anche in caso di assenza non programmata di durata prolungata, a collegarsi al sistema di posta elettronica e ad attivare il risponditore automatico come indicato al punto precedente. In caso di necessità, su specifica richiesta al Responsabile della Struttura competente per i Servizi Infotelematici da parte del responsabile dell'utente assente, o in caso non sia stato possibile raggiungere l'utente assente, verrà incaricato un tecnico informatico il quale procederà all'inserimento del messaggio di assenza dal pannello di controllo del server di posta; all'utente, ed in copia ai dirigenti interessati, verrà inviato un messaggio di conferma dell'attività effettuata. Le specifiche comunicazioni di autorizzazione dovranno essere inviate formalmente via mail.

   Si ricorda in proposito che non è possibile, da parte degli amministratori, accedere alla casella di posta senza conoscere la password, e che pertanto la riservatezza della casella di posta è garantita.

E' vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dal personale tecnico specificamente incaricato, a meno che la cosa non sia stata preventivamente concordata con il Responsabile dell'ufficio Sistemi Infotelematici. In questa casistica sono incluse le mail di progetto stabilite con l'ente in funzione delle esigenze lavorative e concordate con il responsabile che diventano in quel momento uno strumento di lavoro e quindi soggette alle seguenti norme di utilizzo.

Le caselle di posta sono comunque consultabili via web agli indirizzi

http://portal.office.com/

Le caselle di posta elettronica in uso presso l'Ente sono di 2 tipologie:

1) caselle nominative, assegnate con la convenzione:

   <*nome*>.<*cognome*>@ersaf.lombardia.it

   Tali caselle sono intestate personalmente agli utenti: è importante sottolineare che, nonostante le caselle siano intestate ad un individuo, sono da considerarsi uno strumento professionale e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere consono con le funzioni istituzionali svolte dall'Ente. La divulgazione dell'indirizzo di posta nominativo deve essere limitata ai soli casi in cui non possa essere divulgato l'indirizzo di posta relativo all'ufficio di appartenenza.
2) Caselle di posta assegnate ad un ufficio o ad una funzione sul dominio ersaf.lombardia.it. Tali caselle possono essere assegnate ad uno o più utenti. In caso siano assegnate ad un solo utente, questo ha la responsabilità di garantire la continuità nella gestione della corrispondenza; in caso di sua indisponibilità,

programmata o non, dovrà essere attivata una delle 2 differenti modalità per la gestione delle assenze indicate precedentemente. In caso di caselle di posta assegnate a più persone, la continuità nella gestione della corrispondenza e delle attività ad essa correlate dovrà essere assicurata dal relativo Responsabile della Struttura dirigenziale/Unità Operativa a cui tale casella si riferisce, attraverso opportune scelte organizzative.

I tecnici informatici debitamente organizzati, nell'espletamento delle proprie funzioni, potranno accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario della casella (o su sua esplicita autorizzazione), o su richiesta del diretto superiore in caso di indisponibilità dell'assegnatario stesso.

In ogni caso l'Ente di impegna a rispettare la confidenzialità dei messaggi elettronici di provenienza o a destinazione di recapiti sindacali (contenuto, autori e destinatari), delle mailing list elaborate e scambiate in rete da organismi sindacali, ecc.

Al termine del rapporto di collaborazione con l'utente, sulla sua casella verrà attivato un risponditore automatico che segnalerà la cessazione del rapporto e indicherà un indirizzo alternativo istituzionale da contattare in caso di necessità di carattere professionale. I messaggi di posta pervenuti verranno reindirizzati ad un'altra casella, al fine di garantire la continuità delle attività istituzionali.

Alla cessazione del rapporto verrà modificata la password di accesso e, in accordo con il Dirigente responsabile della Struttura di appartenenza dell'utente si deciderà se eliminare la casella o se conservare i messaggi in un archivio *off line* per il tempo necessario.

Per altre indicazioni circa l'utilizzo della posta elettronica si rimanda allo specifico articolo del Codice di Comportamento.

16. Posta elettronica Rappresentanza Sindacale Unitaria

Al fine dell'esercizio del diritto sindacale, ERSAF mette a disposizione:

1) A ciascuno dei delegati RSU, una casella di posta elettronica indicante il cognome e la dizione "RSU". Tramite queste caselle di posta sono diffusi esclusivamente messaggi di carattere sindacale, con l'accortezza di inserire nel testo del messaggio stesso un link che consenta ai soggetti non interessati di comunicare la propria volontà di non ricevere altri messaggi da quella casella di posta.
2) Uno spazio server denominato "BACHECA ELETTRONICA SINDACALE" di capienza pari a 5 GB, gestito esclusivamente dai delegati RSU. I delegati RSU si assumono la responsabilità del contenuto dei documenti inseriti nella BACHECA ELETTRONICA SINDACALE. ERSAF non sarà in alcun modo ritenuta responsabile del contenuto dei documenti in essa pubblicati.

17. Internet

Per lo svolgimento delle proprie mansioni lavorative, agli utenti è garantita la navigazione Internet. Il collegamento ad Internet è uno strumento messo a disposizione per finalità di

carattere lavorativo: è consentita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa a condizione che

- Venga effettuata al di fuori dell'orario di lavoro o durante le pause;
- Non sia contraria alle regole di condotta indicate nel presente codice e non possa in alcun modo ledere l'immagine dell'Ente;
- Non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- Non comporti alcuna violazione di leggi;
- Sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo inappropriato dello stesso.

Pertanto, per garantire quanto previsto dalla legge e secondo le direttive emanate dal Garante per la protezione dei dati personali, al fine di evitare abusi ed evitare il monitoraggio del traffico telematico viene attivato un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali. Il filtro adottato utilizza sistemi euristici di scarto di siti facenti parte di categorie appositamente selezionate. Qualora, per lo svolgimento delle attività istituzionali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiedere per tramite del proprio responsabile (che assumerà la responsabilità di tale richiesta) al Responsabile della Struttura competente per i Servizi Infotelematici l'accesso a tale sito.

È **fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dal personale della Struttura competente per i Servizi Infotelematici.**

È tassativamente vietato effettuare qualsiasi genere di transazione privata in campo finanziario ivi comprese le operazioni di remote banking, acquisti on line e simili fatto salvo i casi di particolare importanza e/o emergenza compatibili con i diritti di conciliazione vita-lavoro.

È tassativamente vietata ogni forma di registrazione e connessione a siti i cui contenuti non siano legati all'attività lavorativa fatto salvo i casi di particolare importanza e/o emergenza compatibili con i diritti di conciliazione vita-lavoro, e comunque mai utilizzando la casella di posta aziendale.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di blog, di bacheche elettroniche e in generale di strumenti di social network anche utilizzando pseudonimi (o nicknames), esclusi gli strumenti autorizzati per esigenze di lavoro.

A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico Internet e dallo scambio di posta elettronica potrà essere soggetta a controlli da parte dell'Ente sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di protezione dei dati personali.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione Internet. Tali controlli saranno preventivamente segnalati al personale e si opereranno secondo stadi successivi:

1) Controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
2) Controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree;
3) Controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

I controlli aggregati e specifici verranno effettuati solo qualora i trattamenti generici non abbiano consentito di risolvere le criticità riscontrate e verranno comunque segnalati in forma preventiva agli utenti.

Tutti i dati di traffico internet potranno comunque essere sottoposti a tracciamento da parte di sistemi automatici implementati presso l'Ente e custoditi per limitati periodi di tempo. La consultazione e conservazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita:

- All'Ente per attività difensive ovvero per far valere o difendere un diritto in sede giudiziaria, come previsto dalla normativa vigente. Qualsiasi trattamento verrà svolto dall'Ente nel rispetto della libertà e della dignità del lavoratore, in osservanza ai principi di pertinenza e non eccedenza;
- Alle forze dell'ordine per attività di carattere ispettivo consentite dalla normativa inerente la protezione dei dati personali.

18. Social Network

Non è consentito l'utilizzo di social network durante l'orario di lavoro, a meno che tali piattaforme non vengano espressamente impiegate in maniera strumentale per lo svolgimento delle proprie attività lavorative.

È assolutamente vietato esprimere opinioni personali su informazioni acquisite durante lo svolgimento delle proprie attività istituzionali o condividere informazioni e riferimenti di carattere professionale che in qualche modo possano ledere l'immagine dell'Ente. Tale divieto è da intendersi anche al di fuori dell'orario di lavoro ed eventualmente oltre la cessazione della collaborazione professionale con ERSAF.
Per qualsiasi danno che potesse derivare all'immagine dell'Ente imputabile a comportamenti non conformi alle indicazioni sopra riportate e comunque contrari alle norme sulla pubblica amministrazione, ERSAF potrà applicare al trasgressore un provvedimento disciplinare ed eventuali sanzioni previste dalla legge.

19. Sicurezza generale e perimetrale

A difesa del sistema informativo dell'Ente è attivato un sistema di sicurezza perimetrale, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.

Il sistema è gestito da Regione Lombardia – LI SpA, che effettua attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, il personale tecnico dedicato verificherà le cause dell'intrusione rilevata, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.

Una volta individuate le cause dell'evento rilevato verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei trattamenti di eventuali violazioni alle regole indicate nel presente disciplinare.

20. Telefonia mobile e dispositivi che consentono la navigazione internet

Tutti i dispositivi di telefonia mobile e/o che consentono la navigazione Internet attraverso un piano tariffario a carico dell'Ente costituiscono uno strumento di lavoro e/o attività istituzionale, pertanto gli eventuali affidatari devono prestare adeguate cautele durante il loro utilizzo.

I dati contabili relativi al traffico telefonico ed Internet potranno essere analizzati dall'Ente al fine di consentire un adeguato controllo e contenimento dei costi. I numeri telefonici presenti nei dati di traffico saranno oscurati nelle ultime tre cifre, per cui non sarà possibile risalire ai numeri contattati. Per quanto riguarda gli aspetti concernenti i consumi telefonici e il traffico Internet generati sui dispositivi si rimanda alle norme comunicate in fase di assegnazione del bene.

Qualora si rilevino delle spese non previste per l'attivazione di servizi eccedenti o utilizzi ulteriori rispetto a quanto indicato precedentemente, l'Ente potrà chiedere all'utilizzatore a cui è stato affidato il dispositivo di evidenziare le voci di spesa personali, al fine di imputargli tale spesa.

L'utente deve fare tutto ciò che è nelle sue facoltà per prevenire eventuali furti di cellulari ed altri dispositivi dati in dotazione, prestando cautela nella loro custodia.

Inoltre, al fine di ridurre il rischio di accesso ai dati residenti sul cellulare da parte di soggetti non autorizzati, l'utente deve attivare sistemi di blocco schermo con protezione con password numerica o con segno grafico composto sullo schermo.

Deve inoltre essere attivato automaticamente il blocco dello schermo entro un massimo di 5 minuti di inattività.

A causa della sempre maggiore interazione tra i dispositivi telefonici e informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi dell'Ente. Pertanto è vietato:

- Utilizzare i dispositivi per navigare in Internet su siti che esulino dalle attività istituzionali;
- Installare applicazioni sui dispositivi cellulari senza prima aver concordato la cosa con la Struttura competente per i Servizi Infotelematici;

- Installare sulle postazioni di lavoro in ufficio programmi di sincronizzazione/backup dei dati contenuti sui dispositivi cellulari senza la preventiva autorizzazione dell'ufficio Sistemi Infotelematici;
- Apportare interventi sulle configurazioni del dispositivo o sulle condizioni di servizio che possano incidere in maniera rilevante sui consumi senza averlo concordato con la Struttura competente per i Infotelematici.

In caso di disservizio o di problemi di funzionamento software, il personale incaricato dal la Struttura competente per i Infotelematici potrà effettuare dei controlli sulla configurazione dei programmi installati sul dispositivo concesso in uso con finalità di protezione del patrimonio aziendale. I controlli verranno effettuati nel rispetto della libertà e della dignità dei lavoratori; il trattamento di eventuali dati personali verrà effettuato nel rispetto dei principi di pertinenza e non eccedenza. Qualora si ravvisino installazioni di programmi il cui funzionamento potrebbe aver danneggiato il patrimonio dell'Ente, il fatto verrà segnalato all'autorità competente che valuterà l'eventuale adozione di provvedimenti disciplinari.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare i dati contenuti sul cellulare (es. Rubrica telefonica, SMS, contenuti multimediali, ecc). Qualora il dispositivo restituito contenga dati personali, questi verranno cancellati indiscriminatamente dal personale incaricato dall'Ente prima di un'eventuale assegnazione successiva.

21. Videosorveglianza

Al fine di tutelare le sedi dell'Ente sono presenti nelle sedi stesse sistemi di videosorveglianza.

La collocazione delle telecamere e gli estremi identificativi delle persone fisiche incaricate del trattamento dei dati, con l'elenco delle funzioni ad essi attribuite, vengono rese note all'interno dell'organizzazione da parte del relativo responsabile del trattamento.

22. Attività dell'Amministratore di Sistema

S'intende per Amministratore di Sistema qualsiasi soggetto le cui funzioni di gestione ed amministrazione di sistemi informatizzati rendano ad esso tecnicamente possibile l'accesso, anche fortuito, a dati personali. In questa definizione rientrano pertanto le funzioni tecnicamente definite di Amministratore di Sistema (*system administrator*), amministratore di base di dati (*database administrator*) o amministratore di rete (*network administrator*).

L'Amministratore di Sistema è designato dal Titolare in forma scritta o designato tramite apposito contratto di servizio stipulato con un Responsabile in outsourcing del trattamento. La designazione quale Amministratore di sistema deve essere conforme alle normative sulla protezione dei dati personali e ai provvedimenti relativi emanati dal Garante della Privacy sull'argomento.

Deve inoltre recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Fra le funzioni dell'Amministratore di sistema, sia esso interno all'Ente che esterno, vi possono essere:

- Sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- Monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- Effettuare e/o coordinare interventi di manutenzione hardware per i dispositivi di competenza;
- Effettuare interventi di manutenzione software su sistemi operativi e applicativi di competenza;
- Coordinare e sovrintendere l'operato di eventuali tecnici esterni a ERSAF (nel caso di Amministratore interno);
- Coordinare a livello operativo la gestione e la distribuzione dei profili di accesso e delle password degli utenti del sistema e/o dei sottosistemi di competenza nel rispetto delle normative relative alla protezione dei dati personali;
- Gestire le password di amministrazione di sistema o dei sottosistemi di competenza;
- Collaborare con i responsabili del trattamento dei dati personali per l'organizzazione delle politiche di sicurezza;
- Informare il responsabile ufficio Sistemi Infotelematici e/o il titolare sulle non corrispondenze con le norme di sicurezza e su eventi di sicurezza rilevanti.

Ai sensi del provvedimento del Garante della Privacy del 2008, sono tracciati i log di accesso degli amministratori di sistema, i quali sono conservati per almeno 6 mesi come previsto dalla normativa.

23. Controlli

Le risorse messe a disposizione dei collaboratori sono strumenti attraverso i quali vengono perseguiti gli obiettivi istituzionali, su cui ERSAF gode di diritti esclusivi di proprietà e utilizzo. Il datore di lavoro ha diritto di ottenere una corretta prestazione lavorativa e di attuare misure di sicurezza idonee alla difesa del patrimonio dell'Ente.

Sulle risorse messe a disposizione dei propri collaboratori, potrebbero essere effettuati dei controlli, con le seguenti finalità:

- Difendere il patrimonio aziendale;
- Far valere o difendere un diritto in sede giudiziaria.

A questi fini, è prevista la possibile attuazione dei seguenti controlli:

- verifica di files e programmi presenti sui dispositivi che contravvengano le indicazioni specificate nel presente codice, con la finalità di prevenire eventuali reati;
- controllo della linea Internet e dei sistemi perimetrali in caso di minacce segnalate dai sistemi di sicurezza o di lentezza di banda, con il fine di garantire il buon

funzionamento della rete aziendale. Il controllo potrà riguardare l'occupazione di banda, l'utilizzo di sistemi di file sharing o la verifica di minacce segnalate dai sistemi di sicurezza;

- controllo della navigazione Internet al fine di prevenzione di possibili minacce che possano compromettere la sicurezza dei sistemi dell'Ente. Il controllo verrà effettuato a seguito della rilevazione di eventi non conformi agli standard di buon funzionamento, e verrà effettuato con profondità graduale come specificato nel precedente capitolo dedicato alla navigazione Internet;
- accesso alla casella di posta degli utenti in caso di loro assenza e di necessità di dovervi accedere per motivi di continuità dell'attività lavorativa. In caso di accesso alla casella di posta, verrà redatto un apposito rapporto di intervento in cui verranno specificate le azioni intraprese, che verrà consegnato all'utente al termine del periodo di assenza;
- analisi del cellulare (o di qualsivoglia altro dispositivo) fornito dall'Ente per motivi di carattere professionale, con finalità di controllo della spesa e protezione dei dati ivi presenti. Le modalità di controllo sono specificate nell'apposito capitolo relativo alla telefonia mobile;
- controllo dell'esito dei backup effettuati sui sistemi server dell'Ente, con la finalità di garantire l'eventuale ripristino di dati o documenti in caso di necessità. Le verifiche potrebbero riguardare il controllo dell'esito dei backup o il ripristino casuale di un dato durante le fasi di test di ripristino effettuate per esaminare il buon funzionamento del sistema;
- controllo della messa in sicurezza dei dati lavorativi residenti sui dispositivi dati in uso, con la finalità di garantire la riservatezza e la disponibilità dei dati dell'Ente. Tale controllo riguarderà la verifica delle misure di backup.

Qualsiasi controllo verrà effettuato nel rispetto della libertà e delle dignità dei lavoratori. Eventuali dati personali rilevati saranno trattati nel rispetto dei principi di pertinenza e non eccedenza.

Qualora da tali controlli si rilevassero dei comportamenti non conformi rispetto a quanto indicato nel presente disciplinare e/o rispetto alle misure di sicurezza definite dall'Ente, ERSAF si riserva il diritto di intraprendere provvedimenti disciplinari.

A seguito di eventi che hanno comportato un danneggiamento al patrimonio aziendale, qualora l'Ente sospetti fondatamente che dei comportamenti di un collaboratore possano aver potuto provocare tale danneggiamento, ERSAF ha diritto di attuare controlli difensivi occulti con la finalità di tutelare il proprio patrimonio, se da tali controlli fosse possibile riscontrare e sanzionare un comportamento idoneo a lederlo.

24. Osservanza del presente codice

La finalità del presente documento è quella di regolamentare l'utilizzo delle risorse informatiche dell'ente, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'Ente.

Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente documento implica la responsabilità personale dell'utente.

I fatti negativi e/o pregiudizievoli espongono il trasgressore oltre che all'apertura di specifico procedimento disciplinare, alle sanzioni previste dalla legge.

25. Osservanza delle regole sulla privacy

Oltre a quanto indicato nel presente documento, è obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali e di misure di sicurezza ICT imposte dalla normativa vigente.

26. Entrata in vigore e aggiornamenti successivi

Il presente documento è in vigore dalla data di adozione dello stesso.

Gli uffici competenti provvederanno a comunicare ai destinatari l'esistenza del presente regolamento, la cui versione più recente potrà in ogni momento essere reperita presso la rete interna aziendale.

E' compito dei collaboratori tenersi al corrente sull'ultima versione disponibile del presente documento attraverso verifica sulla rete interna.

Si pubblica nella Intranet aziendale.

Su raccomandazione espressa dall'Autorità Garante per la Protezione dei Dati personali con propria deliberazione n.13 del 1 marzo 2007, tutti i punti indicati nel presente codice sono stati sottoposti alle Organizzazioni Sindacali con nota di trasmissione prot. ERSAF n. 2017.0016434 del 18.12.2017 per consentire la presentazione di osservazioni entro il 15.01.2018 e al Comitato Unico di Garanzia per le pari opportunità, la valorizzazione del benessere di chi lavora e contro le discriminazioni che lo ha esaminato in data 11.01.2018 inviando le proprie osservazioni al Direttore.