REGIONE EMILIA-ROMAGNA

Atti amministrativi

GIUNTA REGIONALE

Atto del Dirigente DETERMINAZIONE

Num. 8901 del 06/06/2017 BOLOGNA

Proposta:	DPG/2017/9145 del 05/06/2017
Struttura proponente:	SERVIZIO ICT REGIONALE DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI
Oggetto:	APPROVAZIONE DEL DISCIPLINARE PER UTENTI DEI SISTEMI INFORMATIVI DELLA REGIONE EMILIA-ROMAGNA
Autorità emanante:	IL DIRETTORE - DIREZIONE GENERALE RISORSE, EUROPA, INNOVAZIONE E ISTITUZIONI
Firmatario:	FRANCESCO RAPHAEL FRIERI in qualità di Direttore generale

Parere di regolarità amministrativa: PAPILI STEFANIA espresso in data 06/06/2017

'IL DIRETTORE'

Premesso che:

- il processo di riforma avviato dalla L. 124/2015 (Legge Madia) e dal conseguente Decreto legislativo 26 Agosto 2016, n. 179 di riforma del Codice dell'Amministrazione Digitale (Nuovo Cad), pongono in capo ad ogni Ente la necessità di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione, centralizzando in capo ad un ufficio unico il compito di accompagnare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione, con l'obiettivo generale di realizzare un'amministrazione digitale e aperta, dotata di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

- la Legge regionale 24 maggio 2004, n.11, così come modificata con la L.r. 30 luglio 2015 n. 13, "Sviluppo regionale della società dell'informazione", prescrive che siano adottate modalità organizzative finalizzate a garantire la programmazione unitaria e integrata degli obiettivi e delle risorse finanziarie destinate allo sviluppo del Sistema informativo della Regione (SIR-ER) e assegna alla Direzione Generale Risorse, Europa, Innovazione e Istituzioni funzioni di programmazione, sviluppo, coordinamento generale e monitoraggio;

- l'attuazione della legge n. 56/2014, integrata dalla legge n. 190/2014, secondo l'attuazione di cui alla L.R. n. 13/2015, ha comportato, fra l'altro, il passaggio all'organico della Regione e delle sue Agenzie di oltre 1.200 unità di personale, per lo svolgimento delle funzioni oggetto di riordino, con conseguente necessità di adeguamento delle dotazioni, delle infrastrutture regionali per integrare le sedi territoriali e omogeneizzazione dei servizi all'utente;

- la Legge 208/2015 (legge di stabilità 2016) all'art. 1 commi 512-517 fissa norme in materia di programmazione, standardizzazione e razionalizzazione degli acquisti informatici;

Viste le deliberazioni della Giunta regionale:

- n. 2416 del 29/12/2008 "Indirizzi in ordine alle relazioni organizzative e funzionali tra le strutture e sull'esercizio delle funzioni dirigenziali. Adempimenti conseguenti alla delibera 999/2008. Adeguamento e aggiornamento della delibera 450/2007" e in particolare l'Appendice 5 "Trattamento di dati personali con particolare

riferimento alla ripartizione di competenze tra i soggetti che effettuano il trattamento";

- n. 1264 del 01/08/2005 con cui sono state adottate le "Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali";

Vista la deliberazione dell'Ufficio di Presidenza dell'Assemblea legislativa regionale n. 29 del 7/3/2012 "Direttiva e Linee guida dell'Assemblea legislativa della Regione Emilia-Romagna in materia di protezione dei dati personali, con particolare riferimento alla ripartizione di competenze tra i soggetti che effettuano il trattamento. Modifica ed integrazione della deliberazione U.P. n.197/2006. Modifica ed integrazione della Appendice 5 della deliberazione U.P. n. 173/2007";

Visto il Provvedimento del Garante per la protezione dei dati personali "Lavoro: le linee guida del Garante per posta elettronica e internet" del 1 marzo 2007;

Visto il Parere del Gruppo di lavoro sulla protezione dei dati – Articolo 29 "Parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro" del 13 settembre 2001;

Dato atto che con propria determinazione n. 14852 del 17 novembre 2011 è stato adottato il "Disciplinare Tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna";

Considerato che la Regione Emilia-Romagna, nel percorso di informatizzazione e digitalizzazione intrapreso, si propone di utilizzare sempre nuove risorse e servizi tecnologicamente avanzati, al fine di raggiungere maggiori livelli di efficienza ed economicità in un contesto di sicurezza informatica crescente;

Considerato che in questi ultimi anni l'innovazione tecnologica si è notevolmente e velocemente sviluppata e che in virtù della stessa si sono potute approfondire esperienze e conoscenze ulteriori che permettono di individuare misure idonee e preventive atte a ridurre i rischi di distruzione o perdita anche accidentale dei dati utilizzati dall'ente, di accesso non autorizzato o di trattamento non consentito;

Richiamata la deliberazione della Giunta Regionale n. 1718 del 24/10/2016 "Indirizzi per la Governance dell'ICT regionale e Piano di sviluppo 2017-2019" che ha fissato nuovi indirizzi, obiettivi e azioni da sviluppare nel triennio per garantire lo sviluppo dei propri sistemi informativi nel

rispetto dei principi di economicità, efficienza e sicurezza complessiva e che, in particolare, demanda al Servizio ICT Regionale la " predisposizione e promozione di tutti i disciplinari relativi alle politiche di sicurezza e corretto utilizzo dei sistemi informatici ed informativi";

Considerato che:

- il Servizio ICT Regionale ha avviato negli ultimi anni un percorso di certificazione con riferimento all'Area della Sicurezza informatica che si è concluso con il rilascio della Certificazione ISO 27001 in data 26/5/2017;

- nel corso del processo per la Certificazione ISO 27001 sono state evidenziate alcune modalità di gestione delle informazioni e delle strumentazioni, considerate idonee per dare maggiore sicurezza ed efficienza al sistema informativo regionale;

Ritenuto pertanto che sussista la necessità di aggiornare le disposizioni vigenti adottando un nuovo Disciplinare che risponda agli obiettivi, ai programmi e alle azioni precedentemente richiamati;

Vista la proposta elaborata dal Servizio ICT Regionale allegata al presente provvedimento e ritenuto che sia meritevole di approvazione;

Dato atto che il disciplinare allegato al presente provvedimento risulta coerente e pienamente compatibile con i principi già fissati dall'Assemblea per la gestione delle proprie strumentazioni informatiche e per i propri utenti nel "Disciplinare tecnico per gli accreditamenti" approvato con Delibera dell'ufficio di Presidenza n. 132/2013 e nel "Disciplinare tecnico per l'assegnazione delle attrezzature alle Strutture Speciali" approvato con Delibera dell'ufficio di Presidenza n. 108/2014;

Valutata l'opportunità di prevedere decorrenze differenziate per l'entrata in vigore di alcune disposizioni previste nel disciplinare che necessitano di tempi tecnici di adeguamento dei sistemi o un'adeguata informazione agli utenti;

Dato atto che le linee di revisione più importanti del Disciplinare sono stata presentate ai componenti dell'ICT-Com nella seduta del 22/2/2017 e il testo in bozza è stato trasmesso ai singoli componenti per eventuali emendamenti in data 04 maggio 2017;

Acquisito il parere favorevole espresso dal Direttore Generale dell'Assemblea legislativa, con nota prot. PG/2017/418190 del 06/06/2017;

Dato atto di aver rispettato le vigenti disposizioni in materia di relazioni sindacali con deposito effettuato in data 04 maggio 2017;

Dato atto del parere allegato;

D E T E R M I N A

1. di approvare il "Disciplinare per utenti dei sistemi informativi della Regione Emilia-Romagna" allegato al presente provvedimento sotto la lettera A;

2. di disporre la pubblicazione del Disciplinare su Internos con eventuale adozione di altre iniziative idonee ad assicurare ampia informazione a tutti i collaboratori dell'Ente ed in particolare ai soggetti maggiormente interessati nel processo di applicazione del presente disciplinare tra cui gli amministratori di sistema, i referenti ICT e le Guide Digitali;

3. di disporre, in ragione dell'aggiornamento contenuto nel documento delle attuali disposizioni, la notifica del Disciplinare a tutti gli incaricati del trattamento dei dati personali;

4. di dare atto che il Direttore Generale dell'Assemblea legislativa regionale provvederà a dare attuazione a quanto previsto nel precedente punto 3) per quanto di competenza;

5. di demandare al Responsabile del Servizio ICT Regionale l'adeguamento delle configurazioni tecniche e delle modulistiche necessarie a garantire il rispetto dei principi e delle prescrizioni previste nel Disciplinare;

6. di stabilire per l'entrata in vigore delle disposizioni previste nel Disciplinare quanto segue:

   a. con decorrenza 7/6/2017 saranno applicate le nuove politiche di aggiornamento periodico della password utente che prevedono un rafforzamento dei criteri di complessità delle password stesse;

   b. con decorrenza 7/6/2017 sarà disattivata a tutti gli amministratori del dominio delegati la possibilità di creare manualmente accreditamenti utenti sul dominio regionale; a decorrere dalla stessa data l'unica modalità di accreditamento ammissibile per nuovi utenti sarà quella prevista al paragrafo 4 del Disciplinare;

c. con decorrenza 1/8/2017 cesseranno tutti gli accreditamenti degli utenti attuati con procedure difformi da quelle previste al paragrafo 4 del Disciplinare; entro tale termine per gli utenti attualmente accreditati dovrà essere svolta la procedura prevista al paragrafo 4;

d. con decorrenza 1/8/2017 non saranno più assicurate le attività di recupero dei dati presenti sui dischi locali delle postazioni di lavoro degli utenti in caso di sostituzione/ritiro della postazione di lavoro; spetta ai singoli collaboratori, con l'assistenza della rete dei referenti ICT e delle guide digitali, trasferire preventivamente i dati sul cloud personale già disponibile, da febbraio 2017, per ogni utente;

e. con decorrenza 1/8/2017, non saranno più ammesse richieste di assistenza e/o abilitazione di servizi informatici in forma telefonica e/o mezzi non tracciabili; ogni richiesta di assistenza e/o richiesta di abilitazione a servizi informatici dovrà essere inoltrata all'indirizzo servicedesk@regione.emilia-romagna.it, o tramite equivalente compilazione dei format resi disponibili tramite il catalogo dei servizi ICT regionali, al fine della tracciabilità dell'intervento richiesto;

f. con decorrenza 1/9/2017 dovranno essere adeguati alla gestione tramite MDM di cui al paragrafo 5.3 del disciplinare tutti i dispositivi mobili di proprietà dell'Ente, compresi quelli di proprietà dell'Assemblea legislativa, delle Agenzie e degli Istituti Regionali;

g. entro il 31/12/2017, al fine di garantire le prescrizioni emerse in sede di certificazione ISO 27001, dovranno essere dismessi tutti i dispositivi residuali che operano tramite il sistema operativo Windows XP.

IL DIRETTORE GENERALE

Francesco Raphael Frieri

RegioneEmilia-Romagna

DISCIPLINARE PER UTENTI DEI SISTEMI INFORMATIVI DELLA REGIONE EMILIA-ROMAGNA

INDICE

1 SCOPO ED OBIETTIVI

Il presente disciplinare descrive le regole tecniche ed organizzative da applicare per l'utilizzo di strumentazioni informatiche che accedono al sistema informativo della Regione Emilia-Romagna (di seguito denominata "Ente").

Ai fini del presente disciplinare, si intende per "sistema informativo" il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.

Le disposizioni qui contenute hanno la finalità di ottimizzare l'impiego delle risorse regionali, introdurre regole di corretto utilizzo nel contesto organizzativo dell'ente e ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati e delle informazioni, di accesso non autorizzato o di trattamento non consentito, garantire la disponibilità dei servizi e il rispetto delle norme sul diritto d'autore.

Tutta la modulistica relativa all'applicazione del presente disciplinare è reperibile su Internos nella sezione Modulistica on line.

Quanto riportato nel presente disciplinare non esaurisce tutte le prescrizioni contenute nelle vigenti normative relativamente ad illeciti disciplinari, civili e penali, con particolare riferimento alle violazioni di sicurezza e ai reati informatici.

2 CAMPO DI APPLICAZIONE

Il presente disciplinare si applica a tutti i soggetti che utilizzano i servizi del sistema informativo regionale il cui accesso è consentito tramite accreditamento al sistema di gestione delle identità denominato Active Directory.

A mero titolo esemplificativo, rientrano nel perimetro di applicazione della presente disciplina tutti i collaboratori delle strutture ordinarie e speciali della Giunta Regionale, delle strutture ordinarie e speciali dell'Assemblea legislativa regionale, degli organi di controllo della Giunta e dell'Assemblea legislativa, delle strutture e degli organi di governo delle agenzie e degli istituti regionali, delle società e degli altri Enti convenzionati con la Regione Emilia-Romagna per l'utilizzo dei servizi del sistema informativo regionale che prevedono l'utilizzo del dominio regionale.

Nel testo del presente Disciplinare, quando è indicato il Responsabile della sicurezza, ci si riferisce al Responsabile della sicurezza della Giunta e/o al Responsabile della sicurezza dell'Assemblea legislativa, ciascuno per il proprio ambito di competenza.

Nel seguito del disciplinare, i soggetti di cui sopra sono denominati "utenti".

3 LE DOTAZIONI INFORMATICHE INDIVIDUALI

In relazione al rapporto di lavoro instaurato e alle mansioni affidate, l'Amministrazione assegna agli utenti una postazione di lavoro per l'accesso alla rete regionale e ai servizi del sistema informativo, un insieme di dotazioni software individuali e servizi di stampa, fotocopie e scanner con configurazione predisposta per assicurare la tutela della privacy e la riservatezza dei dati e delle informazioni trattate.

Per utenti esterni che abbiano necessità di accedere ai servizi del sistema informativo regionale l'assegnazione di strumentazione idonea viene valutata congiuntamente dal Responsabile della struttura di assegnazione del collaboratore e dal Servizio ICT regionale.

Nel rispetto del Codice comportamento della Regione Emilia-Romagna e alle prescrizioni contenute nel Disciplinare Tecnico in materia di verifiche di sicurezza e controlli sull'utilizzo dei beni messi a disposizione dall'Amministrazione per lo svolgimento dell'attività lavorativa, ogni utente è responsabile del corretto impiego delle risorse messe a sua disposizione dall'Ente.

3.1 LE POSTAZIONI DI LAVORO

La tipologia e le caratteristiche delle postazioni di lavoro sono stabilite dal Servizio ICT regionale, tenuto conto delle esigenze di lavoro rilevate per gruppi di utenti omogenei, dell'evoluzione tecnologica e del rapporto qualità/prezzo/efficienza delle tecnologie disponibili.

Le postazioni di lavoro hanno caratteristiche minime comuni costituite da:

- un sistema operativo omogeneo e sicuro;
- una dotazione di applicativi individuali di base omogenei e standardizzati;
- un insieme di tecnologie che abilitano all'accesso alla rete regionale e a tutti i servizi applicativi dell'Ente, compresi eventuali certificati e/o dispositivi per il controllo delle identità del dispositivo e dell'utente;
- la possibilità di accesso da parte di amministratori di sistema per l'erogazione dei servizi di assistenza remota e aggiornamento automatico;
- la possibilità di configurare parametri standardizzati ai fini di garantire la sicurezza della postazione stessa.

Le postazioni di lavoro sono protette, in caso di assenza, anche temporanea, tramite la sospensione o il blocco della sessione di lavoro. A tale fine è impostata automaticamente l'attivazione dello screen saver in un periodo di tempo congruo e definito dal Servizio ICT Regionale al fine di impedire la lettura e/o la modifica dei dati presenti a video.

Allo scopo di proteggere dati personali, sensibili e/o giudiziari e la sicurezza delle postazioni di lavoro, è vietato collegare supporti rimovibili o altre tipologie di dispositivi di proprietà dell'utente alle postazioni di lavoro dell'Ente.

3.2 LA DOTAZIONE SOFTWARE DELLA POSTAZIONE DI LAVORO INDIVIDUALE

Ogni postazione di lavoro è dotata di una configurazione base costituita dai seguenti software applicativi individuali:

- una coda di stampa unica per l'accesso ai servizi di stampa;
- un antivirus locale;
- un browser configurato centralmente per l'accesso a tutti i servizi applicativi dell'ente;
- un agente per l'esecuzione su server virtuali di applicazioni client/server e/o applicazioni critiche dal punto di vista dei costi di licenza;
- un servizio di accesso al catalogo dei prodotti applicativi installabili da parte dell'utente;
- un insieme di parametri di configurazione controllati centralmente per garantire la sicurezza della postazione di lavoro e la corretta fruibilità di tutti i servizi applicativi dell'ente e di tutti i servizi internet;
- un insieme di certificati di sicurezza finalizzati a garantire la sicurezza dell'utente tramite identità digitale;

Per tutti i collaboratori contrattualizzati e gli amministratori dell'ente di cui al paragrafo 4.2, la postazione di lavoro è inoltre dotata dei seguenti prodotti e servizi:

- un pacchetto di strumenti di produttività individuale;
- una casella di posta elettronica individuale in cloud;
- uno spazio di archiviazione individuale in cloud.

Per i collaboratori esterni di cui al paragrafo 4.3 la fornitura della dotazione aggiuntiva di cui al capoverso precedente è prevista solo qualora sia previsto nei contratti di fornitura e/o si dimostri l'impossibilità di operare e/o collaborare con le strutture regionali con strumenti alternativi di proprietà dei collaboratori esterni e/o dei loro datori di lavoro.

La postazione di lavoro è configurata e gestita centralmente dal Servizio ICT Regionale nel rispetto del principio di standardizzazione di tutte le postazioni di lavoro regionali.

Le direzioni generali, le agenzie e gli istituti regionali dotati di amministratori di sistema competenti nella gestione della piattaforma di standardizzazione possono richiedere al Servizio ICT il decentramento di parte della configurazione e gestione delle postazioni di lavoro; l'Assemblea Legislativa opera già direttamente per la configurazione e gestione di quelle assegnate alla propria struttura. Le funzioni di configurazione e gestione delle postazioni di lavoro sono esercitate in forma federata nel rispetto dello standard regionale applicando alle postazioni di lavoro configurazioni incrementali a condizione che non riducano i livelli di sicurezza applicate alla postazione di

lavoro. L'installazione di prodotti e/o pacchetto software incrementali da parte dei nodi di distribuzione federati sono ammessi previa verifica di sicurezza del pacchetto stesso e compatibilmente con lo standard regionale. Non sono in alcun caso ammesse piattaforme di gestione delle postazioni di lavoro autonome e/o alternative al sistema centrale.

Ogni utente dell'ente può installare applicazioni locali aggiuntive con una delle seguenti modalità:

- accedendo al catalogo regionale delle applicazioni sicure e certificate dichiarate di utilità generale;
- accedendo al catalogo regionale delle applicazioni settoriali e specialistiche richiedendo l'autorizzazione alla installazione ai responsabili delle piattaforme.

Qualora un'applicazione non sia presente nel catalogo, gli utenti possono avanzare richiesta di inserimento della stessa al Servizio ICT regionale che ne valuta il rispetto dei requisiti di sicurezza, economicità e idoneità funzionale.

Qualora la richiesta riguardi dotazioni software locali o virtuali coperte da licenze onerose, la richiesta di installazione deve essere formulata dal responsabile della struttura con le procedure di cui al paragrafo 4.5.

3.3 I SERVIZI DI STAMPA, FOTOCOPIA E SCANNER

Tutti gli utenti dell'ente possono accedere a tutte le stampanti/copiatrici multifunzione regionali, indipendentemente dalla loro collocazione fisica, gestite dal server centrale di controllo dei servizi di stampa e copia che garantisce i principi di stampa sicura ai fini della privacy e accountability dei costi.

Tutte le stampanti multifunzione sono dotate di lettore badge di riconoscimento gestite del server centrale di stampa. Le operazioni effettuate sono associate all'utente a mezzo di riconoscimento del badge di accesso alla macchina o di inserimento manuale delle credenziali di dominio.

Tali informazioni consentono la riconducibilità di ogni copia/fotocopia eseguita alla struttura di appartenenza dell'utente. Il monitoraggio sull'utilizzo del servizio è demandato al Responsabile della medesima struttura secondo la specifica disciplina prevista nel disciplinare verifiche e controlli.

Le stampanti personali e laser dipartimentali in uso presso le strutture regionali resteranno in uso fino all'esaurimento delle scorte di magazzino. Il servizio ICT provvederà al ritiro delle stampanti inutilizzate e/o guaste che non verranno sostituite.

Verranno mantenute in funzione solo le stampanti laser in dotazione a sportelli aperti ai cittadini e/o a utenti con disabilità certificate.

3.4 CORRETTO UTILIZZO E CONSERVAZIONE DELLE DOTAZIONI DI LAVORO

Le dotazioni informatiche di lavoro, insieme agli accessori fisici e alle dotazioni software individuali, devono essere:

- consegnate ad ogni nuovo utente con la configurazione standard di base aggiornata alla data di consegna;
- utilizzate e conservate con diligenza al fine di ottimizzare l'impiego delle risorse dell'ente, il risparmio energetico e l'impatto ambientale, nel rispetto del presente disciplinare, del codice di comportamento dei dipendenti regionali;
- utilizzate in modo pertinente alle specifiche finalità della propria attività e di quelle della propria organizzazione, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi;
- custodite anche in caso di trasferimento di sede e struttura dell'utente insieme a tutte le altre dotazioni strumentali personali. In caso di trasferimento i referenti ICT sono tenuti ad aggiornare i parametri di configurazione in funzione della sede di destinazione;
- restituite immediatamente in caso di cessazione del rapporto di lavoro e/o collaborazione.
- prive di dati conservati in locale al fine di usufruire del backup automatico dei dati e delle informazioni trattate e di garantire una riduzione dei tempi e dei costi di sostituzione.

I dati e le informazioni trattati devono essere salvati nel cloud personale. In caso di sostituzione o guasto della postazione di lavoro, l'assistenza utenti non effettua operazioni di salvataggio di dati e informazioni salvati sui dischi locali della postazione.

Le dotazioni restituite, ritirate per riparazione o sostituite per aggiornamento della dotazione, vengono immediatamente riconfigurate in modo da cancellare ogni dato preesistente e riportate alla configurazione standard del momento. Le dotazioni riconfigurate vengono consegnate al magazzino delle dotazioni disponibili per altri utenti.

3.5 INTERVENTI SULLE POSTAZIONI DI LAVORO DA PARTE DEL SERVIZIO DI ASSISTENZA UTENTI

Gli amministratori di sistema formalmente designati, possono collegarsi in modalità remota alla postazione di lavoro, allo scopo di assicurare l'assistenza tecnica, la sicurezza e l'operatività, effettuando operazioni di manutenzione e aggiornamento del software installato. Gli interventi sono effettuati dagli amministratori accedendo alla postazione con proprie credenziali e privilegi di amministratore di sistema.

Nei casi in cui l'utente segnala malfunzionamenti per la soluzione dei quali, a scopi diagnostici, è indispensabile impersonare l'utente e accedere con i privilegi allo stesso assegnati, l'intervento viene effettuato, solo su specifica richiesta ed autorizzazione dell'utente stesso.

Tutte le operazioni di collegamento remoto vengono tracciate dai sistemi informatici che registrano, in maniera non alterabile, le seguenti informazioni relative all'intervento effettuato:

- data e ora dell'intervento
- nome utente dell'amministratore di sistema intervenuto
- nome utente del soggetto che ha richiesto l'intervento.

4 LE CREDENZIALI DI IDENTIFICAZIONE INFORMATICA E L'ATTIVAZIONE DEI SERVIZI

In adempimento alle misure di sicurezza previste dalla normativa vigente si delineano di seguito le procedure e le regole d'uso per la gestione e assegnazione delle credenziali di identificazione informatica e le procedure per l'attivazione dei servizi assegnati all'utente.

L'accesso alle strumentazioni informatiche utilizzate per i trattamenti di dati personali è consentito soltanto ai responsabili o agli incaricati formalmente designati per gli specifici trattamenti di dati personali.

4.1 COSA SONO LE CREDENZIALI DI IDENTIFICAZIONE INFORMATICA

L'accesso ai dati trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.

Le credenziali di identificazione informatica consistono in un codice per l'identificazione dell'utente associato a una parola chiave riservata, conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'utente, (che può essere associato a un codice identificativo o a una parola chiave), oppure in una caratteristica biometrica dell'utente (anche questa può essere associata a un codice identificativo o a una parola chiave). Di seguito qualche esempio:

- credenziali di identificazione informatica basate su parola chiave segreta: le credenziali userid+password utilizzate per l'accesso alle risorse di dominio (postazioni di lavoro, server intranet, ecc.) o per l'accesso alle applicazioni con autenticazione non integrata;
- credenziali di identificazione informatica basate su dispositivo in possesso e uso esclusivo dell'utente: le credenziali (userid+carta+pin) utilizzate per l'accesso ad aree riservate tramite smartcard (ad esempio "atti al firmatario", firma digitale ecc.);
- credenziali di identificazione informatica basate su caratteristica biometrica dell'utente: le credenziali (userid+impronta+pin) utilizzate per gli accessi ai dispositivi mobili tramite riconoscimento dell'impronta digitale.

Le credenziali sono costituite da uno "userid" (di norma composto dal cognome per esteso unitamente alla lettera iniziale del nome) e da una password creata inizialmente scaduta. Lo userid viene creato disabilitato. L'utente viene abilitato dall'amministratore di dominio e, prima di poter accedere a qualsiasi risorsa informatica, deve cambiare la password.

4.2 ASSEGNAZIONE DELLE CREDENZIALI AL PERSONALE E AGLI AMMINISTRATORI DELL'ENTE

Il rilascio delle credenziali di identificazione informatica al personale dell'ente - compresi i cococo e il personale comandato o in avvalimento da altre strutture pubbliche presso gli enti del dominio regionale, ai consiglieri e agli amministratori regionali - è contestuale alla procedura di inquadramento giuridico da parte del Servizio regionale competente.

Le credenziali di identificazione informatica sono concesse al personale a seguito di una procedura di accreditamento che prevede il riconoscimento "de visu" del personale.

Al personale viene rilasciato un account e un insieme di credenziali che danno diritto all'accesso ai servizi del dominio dell'Ente, ivi compresa una casella nominativa di posta elettronica regionale.

Le credenziali di identificazione informatica sono associate alla matricola con cui il personale è registrato nell'anagrafica dell'Ente e costituiscono condizione necessaria per l'abilitazione all'utilizzo dei servizi informatici.

Il processo di rilascio delle credenziali informatiche è di competenza del Servizio ICT regionale.

Gli account del personale dell'Ente e degli amministratori cessano con la cessazione della ragione giuridica che ne ha consentito l'attivazione.

Al personale dell'Ente viene anche rilasciato un supporto di riconoscimento a lettura magnetica e/o elettronica e/o a radiofrequenza ai fini del riconoscimento per l'accesso agli uffici regionali, per gli adempimenti previsti nell'ambito della gestione delle presenze e per l'utilizzo delle strumentazioni informatiche.

Tale supporto:

- si configura come documento di riconoscimento personale e come tale deve essere conservato e tutelato dal possessore. Il suo smarrimento e/o la sua manipolazione da parte di terzi deve essere immediatamente denunciato agli organi competenti e la denuncia deve essere trasmessa al Servizio che ne ha richiesto il rilascio per attivare la procedura di annullamento.
- deve essere restituito dal soggetto esterno all'ufficio competente al momento della cessazione dell'attività per evitarne un uso improprio.

4.3 ASSEGNAZIONE DELLE CREDENZIALI A SOGGETTI ESTERNI

Qualsiasi soggetto esterno che debba accedere ai servizi di rete e di dominio direttamente presso le sedi della Regione o accedere tramite VPN da remoto a sistemi della rete interna, indipendentemente dall'inquadramento giuridico e/o dalla forma diretta o indiretta del proprio rapporto di collaborazione, deve essere accreditato tramite il rilascio di una credenziale informatica, di una matricola univoca e di un eventuale supporto di riconoscimento a lettura magnetica e/o elettronica e/o a radiofrequenza.

Per il rilascio della matricola e dell'eventuale supporto di riconoscimento magnetico è necessario che sia formulata richiesta alla struttura competente in materia immatricolazione da parte del responsabile del rapporto di collaborazione corredata dai dati di cui al paragrafo successivo.

Ogni soggetto esterno accreditato viene assegnato alla struttura che ne ha richiesto l'accreditamento e viene distinto con codici di classificazione che identificano il rapporto di collaborazione.

Se per accedere ai servizi del sistema informativo regionale, è necessario accedere ai locali della Regione con continuità, potrà essere rilasciato un supporto di riconoscimento conforme dal punto di vista tecnologico al supporto rilasciato al personale dipendente della Regione Emilia-Romagna.

Tale supporto:

- si configura come documento di riconoscimento personale e come tale deve essere conservato e tutelato dal possessore. Il suo smarrimento e/o la sua manipolazione da parte di terzi deve essere immediatamente denunciato agli organi competenti e la denuncia deve essere trasmessa al Servizio che ne ha richiesto il rilascio per attivare la procedura di annullamento.

- deve essere restituito dal soggetto esterno all'ufficio competente al momento della cessazione dell'attività per evitarne un uso improprio.

Ai possessori delle credenziali di identificazione informatica si applicano le medesime discipline in materia di Sistemi Informativi e privacy che si applicano ai dipendenti dell'Ente.

4.3.1 Classificazione dei soggetti esterni

Ogni soggetto esterno per cui si richiede l'accreditamento con la procedura di cui al paragrafo 4.3 del presente disciplinare sarà classificato in macro categorie che potranno essere ulteriormente articolate in sotto categorie ai fini di una più precisa classificazione funzionale dei soggetti.

L'elenco delle macro categorie viene definito e successivamente aggiornato a cura del Servizio competente in materia di amministrazione e gestione del personale.

4.3.2 Procedura di primo accreditamento dei soggetti esterni

L'accreditamento avviene su istanza di un responsabile di struttura speciale o ordinaria. Per gli Enti dotati di autonomia convenzionati con l'Amministrazione regionale per l'esercizio dei servizi di rete, per responsabile di struttura si intende l'amministratore o il dirigente a cui sono attribuiti poteri di amministrazione e gestione.

L'istanza di accreditamento dovrà riportare per ogni soggetto da accreditare i seguenti dati:

- La struttura regionale presso cui assegnare il soggetto;
- Il responsabile della struttura che avanza richiesta di accreditamento;
- Nome e Cognome;
- Luogo e data di nascita;
- Codice fiscale;
- Email personale;
- Azienda per cui opera il soggetto accreditato (se esiste);
- Inizio del periodo di accreditamento;
- Termine del periodo di accreditamento:
- Macro categoria e sottocategoria in cui classificare il soggetto;
- Riferimento di protocollo all'atto che motiva l'accreditamento (Contratto di fornitura di servizi, Contratto di consulenza, Convenzione con soggetto esterno, tirocinio formativo, lavoro estivo guidato, ecc.. In caso di convenzioni, numero di protocollo della comunicazione con la quale si stabiliscono la tempistica e le date di attivazione e di cessazione del rapporto);
- Eventuale richiesta di rilascio del badge per l'accesso ai locali;
- Fotografia uso tessera qualora sia richiesto il rilascio del badge;

L'istanza prevede la dichiarazione del riconoscimento "de visu" del soggetto da accreditare.

La durata dell'accreditamento non deve superare i termini del rapporto contrattuale del soggetto esterno e non può comunque superare il periodo massimo di 60 mesi.

L'istanza, firmata digitalmente, dovrà essere trasmessa tramite sistema di gestione documentale/protocollo informatico alla struttura competente in materia di Amministrazione e Gestione del personale regionale che provvederà:

- all'inserimento dei dati dell'istanza sul sistema centrale di amministrazione del personale regionale;
- al rilascio di una matricola di identificazione unica del soggetto esterno;
- alla produzione del badge/tesserino di riconoscimento, se necessario e richiesto e comunque in copia singola;

Il collaboratore che riceve il badge deve sottoscrivere ricevuta e l'impegno a restituire il badge alla scadenza del rapporto che ne ha consentito il rilascio.

La struttura che richiede l'accreditamento dovrà curare, alla scadenza del periodo, il ritiro del badge e il suo invio alla struttura competente in materia di Amministrazione del personale regionale.

4.3.3 Procedure di proroga, cessazione anticipata e cessazione ordinaria dell'accreditamento

In caso di proroga dell'accreditamento oltre i termini di scadenza, il Responsabile di struttura che ha avanzato l'istanza di accreditamento dovrà, entro 5 giorni lavorativi antecedenti la scadenza, avanzare richiesta di proroga con le medesime modalità utilizzate in sede di primo accreditamento.

La struttura competente in materia di amministrazione e gestione del personale regionale provvederà alla proroga del soggetto esterno tramite inserimento dei dati relativi sul sistema centrale di amministrazione del personale regionale. Qualora il collaboratore sia dotato di badge di riconoscimento, non sarà necessario provvedere all'emissione di un nuovo badge/tesserino.

Qualora il soggetto cessi l'attività prima della scadenza prevista, il Responsabile della struttura di assegnazione dovrà avanzare istanza di revoca con le medesime modalità utilizzate in sede di primo accreditamento.

La struttura competente in materia di amministrazione e gestione del personale regionale provvederà alla cessazione del soggetto esterno tramite inserimento dei dati relativi sul sistema centrale di amministrazione del personale regionale.

Alla scadenza naturale del rapporto in base al quale è stato rilasciato l'accreditamento o in caso di cessazione anticipata sarà compito della struttura che ha avanzato l'istanza di accreditamento provvedere al ritiro del badge/tesserino di riconoscimento e a trasmetterlo alla struttura competente in materia di gestione e amministrazione del personale.

4.3.4 Conservazione dei documenti relativi alle richieste e variazioni dell'accreditamento

I documenti relativi all'istanza di accreditamento contenenti dati personali, saranno gestiti in formato elettronico all'interno del sistema di protocollo informatico/gestione documentale e saranno soggetti alle misure ivi già stabilite per la protezione dei dati personali.

4.3.5 Decentramento della registrazione di utenti esterni presso strutture regionali con autonomia organizzativa e di bilancio

Le procedure di cui al paragrafo 4.3 sono gestite in forma autonoma da parte dell'Assemblea legislativa con le medesime modalità previste dal presente disciplinare fatto salvo l'adeguamento ai propri modelli organizzativi.

Le strutture regionali dotate di autonomia di bilancio e organizzativa e in possesso delle competenze per gestire le piattaforme di immatricolazione in uso presso la Regione Emilia-Romagna, possono avanzare richiesta di gestione autonoma del processo di registrazione al Direttore competente in materia di organizzazione del personale previo assenso da parte del Servizio Amministrazione e Gestione.

La produzione dei badge/tesserini di riconoscimento sarà in tutti i casi effettuata dalla struttura competente in materia di amministrazione e gestione del personale della Giunta regionale.

4.4 GESTIONE DELLE CREDENZIALI

Ogni credenziale di identificazione informatica si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti, fatti salvi i casi di userid amministrativi utilizzati da amministratori di sistema e di servizi di emergenza o similari in cui vi sia la necessità di consentire l'accesso ai servizi stessi senza conoscere a priori i soggetti che vi devono accedere (es. volontari, personale addetto alla gestione emergenze, vigili del fuoco, ecc.); in quest'ultimo caso la struttura di appartenenza provvede a tenere aggiornato un apposito registro con l'indicazione dei nominativi, degli orari e della postazione da cui il soggetto accede.

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Le credenziali di identificazione informatica alle risorse di dominio e alle applicazioni sono immediatamente disattivate nel caso in cui un soggetto interrompa la sua collaborazione lavorativa con l'Ente.

Le credenziali di identificazione informatica che non sono utilizzate da almeno sei mesi vengono disattivate, salvo quelle utilizzate per la gestione tecnica dagli amministratori dei sistemi informatici e quelle utilizzate per l'accesso ai sistemi e alle basi di dati dalle applicazioni.

4.4.1 PROTEZIONE DELLE CREDENZIALI E AZIONI IN CASO DI FURTO

Ciascun utente è responsabile della sicurezza delle proprie password e deve adottare le necessarie cautele per mantenerle segrete. Le password sono infatti strettamente personali e non devono in nessun caso essere comunicate ad altri.

In caso di furto delle credenziali l'utente è tenuto a seguire le procedure di seguito specificate:

- in caso di furto della componente riservata (password o PIN) è necessario, al primo accesso seguente al furto, cambiare la propria password o pin e contattare il personale preposto alle problematiche di sicurezza informatica (all'indirizzo securityadmin@Regione.Emilia-Romagna.it e cedcons@Regione.Emilia-Romagna.it rispettivamente per Giunta e Assemblea legislativa) per darne immediatamente comunicazione;
- in caso di furto o smarrimento della propria smartcard è necessario richiedere la sospensione immediata del certificato digitale al Certificatore. Si dovrà, poi, sporgere denuncia alle Autorità competenti e trasmettere al Responsabile del Servizio Amministrazione e Gestione la richiesta di revoca del certificato digitale (su apposito modulo) allegando copia della denuncia di furto o smarrimento.

4.4.2 IMPOSTAZIONE DELLE PASSWORD

Ciascun utente quando effettua l'accesso ad un sistema per la prima volta è tenuto a modificare e personalizzare la password di accesso che deve essere lunga almeno 10 caratteri.

Consigli per la corretta impostazione della password

Si raccomanda di:

- non impostare la password in modo che sia facilmente collegabile alla propria vita privata (per es. il nome o il cognome di familiari, la targa dell'auto, la data di nascita, la città di residenza, ecc.).
- non impostare come password parole comuni riportate in un vocabolario (esistono infatti programmi fraudolenti, utilizzati per la forzatura di password che si basano su ricerche sistematiche effettuate sulle parole comuni)
- modulare il grado di complessità della password in funzione del valore dei dati e delle risorse da proteggere; password di account con privilegi amministrativi, per esempio, richiedono complessità superiori rispetto a quelle di account non privilegiati
- scegliere password che contengano combinazioni di lettere maiuscole e minuscole, numeri, caratteri speciali (per esempio !, *, /, ?, #)
- non utilizzare la medesima password su sistemi differenti (per es. scegliere una password di dominio differente da quella impiegata per l'accesso a siti web esterni all'Ente).

4.5 ATTIVAZIONE E REVOCA DI APPLICAZIONI E SERVIZI DEL SISTEMA INFORMATIVO/INFORMATICO REGIONALE

La richiesta di attivazione e revoca dei servizi del sistema informativo/informatico regionale e l'installazione/rimozione dei pacchetti software onerosi è di competenza del Responsabile della struttura a cui l'utente è assegnato.

Ogni richiesta di attivazione e/o abilitazione ai servizi informatici dovrà riportare obbligatoriamente il numero di matricola del soggetto accreditato sul dominio regionale a cui si intende assegnare la risorsa.

La procedura di attivazione e assegnazione di un servizio del sistema informativo/informatico regionale ad un utente accreditato sul dominio regionale risponde ai seguenti requisiti:

1. Il responsabile della struttura assegnataria avanza richiesta in forma scritta e tracciabile, anche in forma dematerializzata, di assegnare un servizio o un pacchetto software oneroso all'utente accreditato;
2. Il servizio tecnico che amministra il servizio informatico richiesto abilita l'utente all'utilizzo del servizio registrando l'evento sulle piattaforme di accreditamento applicativo.
3. L'utente abilitato e il richiedente sono informati dell'avvenuta assegnazione del servizio e/o installazione del pacchetto tramite i sistemi ordinari di notifica.

Al fine di garantire la sicurezza e la responsabilità, il processo di abilitazione è tracciato in tutte le sue fasi sul sistema informatico dell'ente ai fini dell'individuazione della responsabilità di processo.

In caso di cessazione e/o cambio di struttura dell'utente richiedente i servizi assegnati in precedenza sono di norma revocati.

In caso di sostituzione del responsabile di una struttura il responsabile entrante è tenuto a rivedere le assegnazioni di servizi a tutti i collaboratori interni ed esterni della struttura.

Le procedure di accreditamento e assegnazione/revoca dei servizi ICT e dei pacchetti software potranno essere dematerializzate tramite le piattaforme di gestione dei processi digitali regionali nel rispetto dei principi di responsabilità previsti nel presente disciplinare.

5 UTILIZZO DI POSTAZIONI DI LAVORO PORTATILI

Se la dotazione fornita dall'Ente prevede l'utilizzo di computer portatili occorre adottare comportamenti adeguati a prevenire l'accesso da parte di soggetti non autorizzati in ragione della:

- natura dei dispositivi: tali dispositivi sono facilmente trasportabili ed occultabili;
- natura dei dati presenti sui dispositivi: sui dispositivi mobili possono essere presenti copie parziali e/o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;
- modalità di utilizzo dei dispositivi: possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Ente ed in aree non sicure e ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui ci si riconnette alla rete interna.

5.1 PREVENZIONE E SALVAGUARDIA DEI DATI

Per quanto sopra precisato è fatto divieto ad ogni utente di salvare in locale credenziali che consentano l'accesso alla rete o ad applicazioni dell'Ente.

Suggerimenti per evitare accessi non autorizzati ai dati e ai servizi dell'Ente

Si raccomanda di:

- provvedere, al momento della riconnessione alla intranet regionale, al salvataggio su unità di rete o sul proprio disco personale in cloud di eventuali file copiati o creati in locale, rimuovendoli dal dispositivo mobile
- memorizzare in forma protetta i file che contengono dati sensibili e/o giudiziari (per es. proteggere l'accesso a cartelle o file tramite password, utilizzare appositi strumenti di cifratura concordandoli con il proprio referente informatico o con le strutture informatiche centrali, ecc.)
- distruggere i supporti rimovibili contenenti dati sensibili e/o giudiziari, o rendere inintelligibili i dati in essi contenuti, impiegando strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali

5.2 PREVENZIONE E SALVAGUARDIA DELLE POSTAZIONI DI LAVORO PORTATILI

Per prevenire furto, danneggiamento involontario e comunque situazioni di pericolo relative all'integrità dei dispositivi e dei dati, in ragione della portabilità degli stessi, l'utente è tenuto a:

- custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio, ecc.);
- durante il trasporto osservare le istruzioni del fabbricante per la protezione dei dispositivi da urti, campi elettromagnetici e sbalzi di temperatura;
- trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
- non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;
- non lasciare i dispositivi in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno;
- non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli

in cassaforte se si prevede un'assenza prolungata.

I computer portatili ad uso individuale devono essere utilizzati esclusivamente dall'utente a cui gli stessi sono stati assegnati e, qualora siano assegnati alle strutture, il loro utilizzo deve essere regolamentato dalle stesse, in funzione delle proprie peculiarità ed in modo tale da garantirne il controllo.

Gli utenti assegnatari provvedono al collegamento delle postazioni di lavoro portatili alla rete dell'Ente almeno una volta ogni 30 giorni per effettuare gli aggiornamenti automatici del software antivirus e delle patch di sicurezza del sistema operativo e di tutti i prodotti software installati. Se l'utente assegnatario utilizza il dispositivo mobile per telelavoro, lo stesso è tenuto ad osservare le disposizioni illustrate nel paragrafo relativo.

5.3 UTILIZZO DI SMARTPHONE E TABLET FORNITI DALL'ENTE

I dispositivi mobili, in ragione della loro natura, rappresentano una minaccia rilevante alla confidenzialità dei dati e delle informazioni dell'Ente. Specificatamente i dispositivi mobili sono soggetti a rischi specifici quali perdita di informazioni, accesso a dati "sensibili", facilità di furto, accesso a reti wireless non sicure, possibilità di download di app con contenuto malevolo.

La gestione dei dispositivi mobili assegnati dall'Ente a collaboratori e amministratori da parte del personale del Servizio ICT o da parte di Direzioni, Assemblea legislativa, Agenzie e Istituti espressamente autorizzati a fornire dispositivi mobili, avviene attraverso uno strumento di Mobile Device Management (MDM) centralizzato. Il sistema MDM ha lo scopo di monitorare la sicurezza di tali dispositivi e di determinare centralmente il rispetto di parte delle policy qui descritte.

Per ridurre il livello di esposizione alle minacce viene stabilito che:

- Ogni utente che riceve in dotazione un dispositivo mobile è responsabile del suo corretto utilizzo.
- È fatto divieto di effettuare la disinstallazione o disattivazione dell'agente MDM dal dispositivo mobile da parte degli utenti.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'ente, attraverso il sistema MDM, attiva automaticamente l'impostazione del blocco dello schermo dopo pochi minuti di inattività (interazione utente-device) con sblocco attraverso password, pin o riconoscimento biometrico.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'ente, attraverso il sistema MDM, installa sul dispositivo mobile un software anti malware il cui database è aggiornato continuamente (database definizione virus).
- È fatto divieto all'utente di effettuare la disinstallazione, la disattivazione o qualsiasi manipolazione del software anti malware installato; l'utente inoltre è tenuto a consentire l'aggiornamento del software anti malware attraverso la connessione dati.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'ente rileva tramite il sistema MDM il software installato autonomamente dall'utente. Nel caso in cui il software installato comporti rischi per la sicurezza, l'utente viene invitato a rimuoverlo dal dispositivo.
- È fatto divieto di modificare funzionalità del sistema operativo del dispositivo mobile attraverso operazioni di "rooting" o "jailbreaking".
- L'accesso via VPN alla rete regionale attraverso il dispositivo mobile deve essere esplicitamente autorizzata dal Servizio ICT Regionale.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile, sia all'interno che all'esterno degli uffici regionali, riponendolo in cassetti o armadi chiusi a chiave in caso di non utilizzo.
- In caso di furto o smarrimento del dispositivo, l'utente è tenuto a segnalarlo tempestivamente al servizio che gestisce il dispositivo, in modo che gli incaricati della gestione dei dispositivi mobili dell'ente provvedano alla cancellazione remota dei dati contenuti all'interno ("remote wiping"); l'utente deve inoltre effettuare la denuncia presso le autorità competenti e far pervenire una copia della denuncia al servizio che gestisce il dispositivo mobile.

- Poiché i dispositivi mobili sono utilizzati su reti di cui l'Ente non ha nessun controllo, con conseguente rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi, l'utente è invitato ad utilizzare reti Wi-Fi con accesso tramite autenticazione.
- Il personale tecnico addetto alla gestione dei dispositivi mobili dell'ente è tenuto ad effettuare un audit periodico delle attività effettuate dagli utenti possessori di dispositivi mobili, allo scopo di individuare accessi non autorizzati ai dati, violazioni delle policy e compromissioni dei dispositivi. Tale audit viene effettuato senza alcuna comunicazione preventiva all'utente, nell'interesse della tutela del patrimonio informativo dell'Amministrazione e della sicurezza delle informazioni degli utenti.
- Salvo specifica richiesta dell'Autorità giudiziaria la funzione degli strumenti di MDM che consente il tracciamento della posizione fisica in cui si trova il dispositivo (geo localizzazione), è disattivata.

5.4 TELELAVORO

Ai collaboratori regionali con rapporto di lavoro a distanza viene consegnata una postazione di lavoro interconnessa alla Intranet regionale: l'utente può quindi accedere, anche dalla propria abitazione, a tutti i dati e servizi a cui accede normalmente in ufficio.

La postazione di telelavoro è installata, configurata e mantenuta dal Servizio ICT Regionale o da una eventuale struttura ICT decentrata.

L'utente in telelavoro è tenuto:

- ad utilizzare la postazione di lavoro fornitagli esclusivamente per motivi inerenti l'attività lavorativa;
- a rispettare le norme di sicurezza indicate nel presente disciplinare;
- a non manomettere in alcun modo gli apparati e l'impianto generale;
- a non variare la configurazione della postazione di telelavoro;
- a non sostituirla con altre apparecchiature o dispositivi tecnologici.

Per evidenti ragioni di sicurezza tale postazione non può essere impiegata con collegamenti alternativi o complementari a quello installato/autorizzato dall'Ente ed il suo utilizzo non può essere consentito ad altri soggetti all'infuori del telelavoratore.

In attuazione di quanto previsto nella disciplina del telelavoro, nel caso in cui non sia possibile attivare l'interconnessione standard alla Intranet regionale o vi sia urgenza dell'attivazione del telelavoro (esempio stato di salute o assistenza handicap), il telelavoratore viene abilitato all'accesso attraverso il servizio di Virtual Private Network (VPN) messo a disposizione dall'Ente, utilizzabile con ogni tipo di collegamento ad Internet (Internet key, ADSL flat, ecc.). in tal caso l'utente è tenuto a:

- collegarsi dal PC del telelavoro via VPN ogni qualvolta deve accedere alla rete regionale
- provvedere al collegamento del computer portatile ad una presa di rete interna presso il proprio ufficio almeno una volta ogni 30 giorni per consentire gli aggiornamenti automatici del software antivirus e delle patch di sicurezza.

5.5 UTILIZZO DEI DISPOSITIVI NON FORNITI DALL'ENTE

I soggetti accreditati al dominio regionale hanno accesso ai servizi dell'Ente esposti sulla rete esterna o resi disponibili in modalità cloud, pertanto fruibili attraverso una pluralità di dispositivi.

Al fine di mantenere la sicurezza dei dati di proprietà dell'Ente trattati attraverso tali dispositivi è necessario che l'utente adotti gli accorgimenti e gli strumenti necessari per garantire la riservatezza, l'integrità e la disponibilità dei dati memorizzati sull'infrastruttura informatica dell'Ente, prevenendone la memorizzazione insicura ovvero la loro trasmissione attraverso una rete insicura, dove possono essere facilmente compromessi. Obiettivo di queste disposizioni è anche la tutela dell'utente stesso, che adottando i comportamenti indicati non incorre in violazioni delle normative vigenti e nel riconoscimento di responsabilità.

L'utente che accede ai servizi aziendali fuori dalla rete regionale è tenuto a:

- non memorizzare dati dell'Ente su dispositivi personali, soprattutto nel caso di documenti classificati come "confidenziali" o "strettamente confidenziali" e nel caso di presenza di dati personali (in particolare se sensibili

o giudiziari) e a non scaricare in locale gli allegati di posta elettronica. Nel caso in cui i dati dell'Ente venissero inavvertitamente salvati sul dispositivo personale, l'utente è tenuto a cancellarli immediatamente dal dispositivo;
- impostare il blocco automatico dello schermo del dispositivo dopo pochi minuti di inattività (interazione utente-device) con sblocco attraverso password, pin o riconoscimento biometrico;
- installare sul dispositivo un software anti malware con aggiornamento costante del database di definizione dei malware (a titolo esemplificativo Avast, Malwarebytes, Avira, AVG);
- utilizzare in via esclusiva il dispositivo configurato per l'accesso a dati dell'Ente, quindi senza condividerne l'utilizzo con altri soggetti, compresi i propri familiari;
- mantenere aggiornato il dispositivo, applicando tutte le patch di sicurezza, upgrade del sistema operativo e aggiornamenti delle applicazioni installate;
- non installare sul dispositivo applicazioni provenienti da fonti non ufficiali e/o potenzialmente pericolose per l'integrità e la sicurezza dei dati dell'Ente;
- non utilizzare sul dispositivo lo stesso client per accedere sia alla posta elettronica aziendale che a quella personale ovvero per accedere ai documenti dell'Ente disponibili in cloud.

5.6 UTILIZZO DI SMARTPHONE E TABLET PERSONALI PER L'ACCESSO A DATI E SERVIZI DELL'ENTE

È possibile accedere ad alcune delle risorse dell'Ente a mezzo di smartphone e tablet anche di proprietà personale, sia nel caso in cui la SIM card sia di proprietà personale, sia nel caso in cui la SIM card sia fornita dall'Ente.

Per questi casi, oltre a quanto già prescritto nel paragrafo precedente, si stabilisce che:

- I protocolli consentiti per l'accesso alla posta elettronica da smartphone e tablet sono: MAPI e Microsoft Exchange ActiveSync;
- La configurazione dell'account aziendale sull'app nativa per la gestione della posta elettronica è subordinata all'accettazione del fatto che il sistema di gestione del servizio di posta elettronica regionale, per funzionare, necessita di acquisire il controllo del dispositivo al fine di poter attuare attività avanzate di gestione, anche remota, del dispositivo mobile. Tra gli strumenti avanzati per la gestione remota si segnala la possibilità – in caso di furto o smarrimento - di effettuare il "remote wiping". Questo consente di rimuovere i contenuti personali ed aziendali dal dispositivo rubato o smarrito. L'operazione viene svolta direttamente dall'utente con il supporto assistito dello staff tecnico del servizio ICT Regionale o dell'Area informatica dell'Assemblea legislativa.
- L'utente è tenuto ad impostare il blocco automatico dello schermo dopo pochi minuti di inattività con sblocco attraverso password, pin o riconoscimento biometrico. Nel caso di dispositivi mobili personali con SIM di proprietà dell'Ente, tale blocco è impostato centralmente dagli amministratori del servizio ICT Regionale.
- Come indicato nel paragrafo precedente l'utente è tenuto ad installare sul proprio dispositivo mobile un software antimalware. Nel caso di SIM di proprietà dell'Ente, sul dispositivo mobile personale il software antivirus è fornito dall'Amministrazione.
- L'utente è tenuto a non installare app al di fuori dei canali di distribuzione ufficiali (Google Play, Microsoft Store o Apple Store) e a non installare app non compatibili con la sicurezza dei dati.
- Al fine di evitare il furto dei dispositivi, con conseguente pericolo di accesso ai dati contenuti all'interno, l'utente è tenuto a non lasciare incustodito il dispositivo mobile.
- L'utente deve inoltre effettuare la denuncia presso le autorità competenti e far pervenire una copia della denuncia al Servizio ICT Regionale o all'Area informatica dell'Assemblea legislativa.
- Nel caso in cui l'utente sospetti una violazione dei dati dell'Ente, la presenza di un malware, oppure la compromissione del proprio dispositivo mobile personale utilizzato per accedere a dati dell'Ente, è tenuto a segnalarlo tempestivamente all'assistenza utenti del Servizio ICT Regionale o all'Area informatica dell'Assemblea legislativa, in modo che, se fosse confermata una compromissione di dati dell'Ente, possano essere attivate opportune contromisure al fine di limitare i danni.
- Poiché i dispositivi mobili sono utilizzati su reti di cui l'Ente non ha nessun controllo, esiste un rischio di intercettazione e/o di modifica delle comunicazioni effettuate con tali dispositivi. Per tali motivi l'utente è invitato ad utilizzare preferibilmente reti Wi-Fi con accesso tramite autenticazione.

6 UTILIZZI DELLA RETE REGIONALE

Al fine di prevenire l'accesso ai sistemi informatici da parte di soggetti non autorizzati è fatto divieto di:

- connettere ad Internet, tramite reti wi-fi, modem o altri apparati di accesso remoto non espressamente autorizzati, strumentazioni informatiche collegate alla rete interna dell'Ente;
- connettere alla rete interna dell'Ente strumenti elettronici personali o comunque non espressamente autorizzati;
- connettere alla rete interna dell'Ente access point o altri apparati di rete non espressamente autorizzati;
- installare e/o comunque utilizzare software peer-to-peer o utilizzare le postazioni di lavoro collegandole tra loro per la condivisione di file e stampanti;
- utilizzare strumenti di sniffing, cracking o scanning e introdurre o diffondere volontariamente programmi nocivi (per es. virus, worm, spyware, ecc.) nella rete o nei sistemi.

7 POSTA ELETTRONICA

La casella di posta elettronica viene fornita dall'Ente quale strumento di supporto per lo svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa.

Le caselle di posta elettronica sono assegnate come servizio di base:

- a ciascun dipendente e amministratore al momento dell'inquadramento giuridico;
- a ciascuna struttura regionale al momento della sua istituzione;

Ai collaboratori esterni accreditati al dominio regionale la casella di posta è assegnata su richiesta motivata del Responsabile della struttura qualora risulti indispensabile per svolgere attività che non risulta possibile svolgere con email personali e/o aziendali. La richiesta di attivazione dei servizi di posta personale regionale ai collaboratori esterni accreditati segue le procedure di cui al paragrafo 4.5.

L'attivazione di ulteriori caselle di posta elettronica, per attività di gruppo o di progetto, può essere richiesta al Servizio ICT Regionale dal Responsabile di struttura o da un suo delegato con le procedure di cui al paragrafo 4.5.

Le caselle di posta elettronica certificata (PEC) non sono di norma nominative, ma assegnate alle strutture regionali per le quali sono previsti processi di comunicazione istituzionale con soggetti terzi. Solo in casi particolari e documentati possono essere richieste al servizio ICT Regionale PEC nominative. La richiesta di attivazione di caselle PEC segue le procedure di cui al paragrafo 4.5.

Al fine di assicurare la disponibilità dei dati e delle informazioni pervenute o inviate dalle caselle di posta elettronica si raccomandala creazione e l'utilizzo di caselle di posta elettronica di struttura e/o di progetto condivise tra gli utenti che concorrono alle suddette attività.

L'amministrazione degli utenti che accedono a caselle di struttura, di gruppo o di progetto è assegnata ai responsabili delle strutture regionali o a loro delegati.

La casella di posta elettronica personale rientra tra gli strumenti assegnati agli utenti del sistema informativo regionale.

L'accesso al contenuto della casella di posta elettronica personale è consentito solo all'utente assegnatario. L'accesso da parte di terzi alla casella personale di un utente è vietato salvo quanto indicato nel paragrafo 13. È inoltre fatto salvo l'eventuale adempimento a richieste dell'Autorità giudiziaria. Nel caso di specifica e circostanziata segnalazione relativa ad un utilizzo improprio di una casella di posta istituzionale, l'accesso può essere effettuato, allo scopo di evitare la distruzione di informazioni necessarie per lo svolgimento di un procedimento disciplinare, su richiesta del soggetto titolare del procedimento stesso.

7.1 UTILIZZO DELLA POSTA ELETTRONICA

La posta elettronica deve essere utilizzata esclusivamente per le specifiche finalità della propria attività lavorativa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi e degli altri utenti regionali e dei processi lavorativi, adottando comportamenti idonei a prevenire la perdita di confidenzialità di dati riservati e l'utilizzo non appropriato di beni dell'Ente.

La casella di posta elettronica certificata (PEC) e quella ordinaria sono mezzi attraverso i quali è possibile la trasmissione di dati personali. Nei casi in cui siano utilizzati quali mezzi per trasmettere dati personali a soggetti terzi, si rammenta che tale operazione costituisce comunicazione di dati personali e, come tale deve essere effettuata ai sensi della normativa vigente, oppure a riscontro di una istanza dell'interessato ai propri dati personali.

Nel caso di utilizzo della posta elettronica certificata (PEC) per la trasmissione di dati personali comuni (vale a dire non sensibili e/o giudiziari) il cui trattamento sia di titolarità dell'Ente, l'utente dovrà solo accertarsi della legittimità del destinatario a ricevere i dati personali che intende inviare; qualora venisse utilizzata, invece, la casella di posta elettronica "ordinaria" l'utente dovrà accertarsi, oltre che della legittimità del destinatario alla ricezione dei dati personali, anche dell'identità dello stesso, che si intende certa se:

- ha presentato via email una richiesta per l'invio dei dati firmata digitalmente;
- ha inviato, oltre alla richiesta di dati presentata via email o telefonicamente, anche una copia semplice di un documento di identità in corso di validità (anche tramite email o fax).

Nel caso di ragionevole certezza sull'identità del richiedente (ad esempio perché il richiedente è conosciuto personalmente) ovvero in casi di improrogabile urgenza, l'accertamento sull'identità del ricevente può essere effettuata per via telefonica.

Le modalità tecniche cambiano in relazione alla tipologia dei dati personali che si intende inviare.

Nei casi in cui sia necessario inviare dati personali sensibili e/o giudiziari, rilevata da parte dell'utente la liceità del trattamento ai sensi della normativa vigente, la comunicazione deve essere effettuata secondo una delle seguenti modalità:

- utilizzando opportune tecniche di cifratura avvalendosi di strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali;
- impiegando soluzioni alternative che rendano i dati temporaneamente inintelligibili e permettano di identificare gli interessati solo in caso di necessità (per es. mandare in email separate i dati sensibili/giudiziari dagli altri dati personali, utilizzare codici identificativi al posto di nome e cognome, ecc.).

7.2 SUGGERIMENTI PER LA PREVENZIONE DA MALWARE

Al fine di prevenire le minacce rappresentate da software malevoli (per es. virus, worm, spyware, ransomware ecc.) che potrebbero essere contenuti in email o negli allegati delle email stesse, si forniscono le seguenti indicazioni:

1. "Spam" è il termine con cui si indica l'invio incessante, ma soprattutto indesiderato di messaggi pubblicitari o parti delle cosiddette catene di S. Antonio ad un gran numero di utenti contemporaneamente. Le operazioni di invio possono realizzarsi via email o tramite i gruppi di discussione. A titolo preventivo si raccomanda di:

- non rispondere mai a messaggi di presunto spamming, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
- limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail su siti web pubblici (per es. forum, mailing list, ecc.);
- non rispondere o inoltrare email di c.d. "Catene di S. Antonio", ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
- non configurare la conferma di lettura in modalità automatica.

2. Il phishing è una tecnica di attacco che sfrutta email e siti web "fantasma", del tutto simili nell'aspetto agli originali, per ingannare l'utente e carpire informazioni confidenziali o personali. È necessario, quindi, prestare massima attenzione alle email che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi quali Yahoo!, Postecom, ecc.).

3. In caso di dubbi sulla qualità di messaggi email, si raccomanda di contattare l'indirizzo di posta dedicato alle problematiche di sicurezza informatica (securityadmin@regione.emilia-romagna.it e cedcons@Regione.Emilia-Romagna.it rispettivamente per Giunta e Assemblea legislativa*)*.

8 NAVIGAZIONE IN INTERNET

L'Ente fornisce l'accesso ad Internet a supporto dello svolgimento dell'attività lavorativa e delle attività che siano strumentali e connesse alla stessa e per questo se ne prescrive un utilizzo pertinente alle specifiche finalità, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.

È fatto divieto di:

- modificare le configurazioni standard del browser web fornito dall'Ente;
- accedere a caselle web mail di posta elettronica personale forniti da provider che non assicurano strumenti di protezione adeguati;
- scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, verificare la provenienza e l'autenticità del software (per es. tramite meccanismi di firma digitale);
- utilizzare siti pubblici di condivisione dei file e di archiviazione online forniti da provider che non assicurano strumenti di protezione adeguati;
- caricare documenti inerenti l'attività lavorativa o istituzionale, soprattutto se contenenti dati personali, sensibili e/o giudiziari, su siti pubblici di condivisione, archiviazione o backup online;
- utilizzare siti che permettano di usufruire di web proxy pubblici, aggirando l'obbligo di utilizzo del web proxy dell'Ente per la navigazione

Viste le nuove tipologie di attacco che hanno sempre più per oggetto l'utente finale e come mezzo di propagazione il web o la posta elettronica, e visto che la sempre più le comunicazioni web utilizzano canali cifrati, il personale del Servizio ICT addetto alla sicurezza informatica è autorizzato a configurare i sistemi di sicurezza dedicati alla navigazione web affinché venga ispezionato il traffico cifrato per alcuni siti ritenuti ad alto rischio, tipicamente quelli che permettono lo scambio di documenti, allo scopo di individuare e bloccare eventuale malware o strumenti di attacco. Tale ispezione, funzionale unicamente alla verifica della sicurezza delle informazioni, è effettuata con strumenti automatici; per nessun motivo viene utilizzato per il controllo dell'attività lavorativa.

9 PROTEZIONE ANTIVIRUS

L'utente utilizzatore delle risorse informatiche dell'Ente è tenuto ad adottare le necessarie cautele al fine di ridurre il rischio di infezione virale della propria o altrui postazione di lavoro. È fatto quindi divieto, ai soggetti che sono amministratori di postazione di lavoro, di rimuovere il programma antivirus installato su di essa e di alterarne la configurazione. Si invitano gli utenti a segnalare tramite ticket problemi eventualmente riscontrati sulla corretta installazione e funzionamento del programma antivirus installato sulla propria postazione di lavoro.

Si raccomanda, inoltre, prima di utilizzare supporti rimovibili, di verificare la presenza di eventuali virus in esso contenuti.

A seguito di segnalazione della presenza di un virus da parte del software antivirus si prescrive di:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare tramite ticket l'evento alla struttura di Service Desk competente;

- non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti.

10 GESTIONE DEI LOG

I sistemi informativi dell'Ente sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti, ed in particolare dei requisiti di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali, secondo le modalità contenute nel relativo disciplinare.

Alcune attività dell'utenza sono soggette a *logging*: ciò significa che alcune operazioni eseguite dagli utenti di sistemi informativi vengono memorizzate in formato elettronico e conservate per un certo periodo di tempo. Il *logging* è necessario per ragioni di sicurezza: il livello del *logging* dei diversi servizi, ossia il livello di dettaglio dei dati memorizzati, è funzionale unicamente alla verifica della sicurezza con la quale i servizi sono erogati e all'applicazione del Disciplinare Tecnico sopra citato; per nessun motivo viene utilizzato per il controllo dell'attività lavorativa.

Di seguito vengono dettagliate le tipologie di log raccolti e conservati:

- log della navigazione web, del firewall e del server di posta: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze; scopo ulteriore della raccolta, per quel che riguarda la navigazione web, è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Ente al fine di svolgere la propria attività lavorativa;
- log delle segnalazioni ed alert di tutte le tipologie di sistema antimalware: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli amministratori di sistema ai sistemi amministrati: tale raccolta è motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema;
- log degli accessi degli utenti ai servizi di rete: tale raccolta deriva dalla necessità di poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli utenti al sistema di stampa e delle operazioni effettuate: tale raccolta deriva dalla necessità di poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze; scopo ulteriore della raccolta è quello di verificare il corretto utilizzo delle strumentazioni assegnate dall'Ente al fine di svolgere la propria attività lavorativa;
- log delle attività svolte da utenti e amministratori di sistema nell'ambito di alcuni software complessi: tale raccolta è motivata dalla necessità di poter individuare anche a posteriori eventuali violazione delle policy e audit sulla correttezza dei dati gestiti dal software stesso.

Il tempo di conservazione di tutte le tipologie di log sopra elencate è fissato ad un periodo di un anno. Ciò è motivato dalla necessità di utilizzare tali log per la verifica annuale delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema e di avere una policy di retention dei log uniforme per tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.

11 PREVENZIONE E GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Al fine di prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile è di enorme rilevanza operare tempestivamente e in uno spirito di collaborazione.

Qualora si ravvisassero violazioni di sicurezza interna o eventi che possano portare a credere che vi sia stata un'elusione delle misure di sicurezza previste, è di fondamentale rilevanza segnalare tempestivamente l'accaduto al responsabile funzionale o al referente ICT di riferimento.

In un'ottica di prevenzione degli incidenti di sicurezza, è necessario attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna dell'Ente.

12 PROTEZIONE DEI DATI TRATTATI SENZA L'UTILIZZO DI STRUMENTI ELETTRONICI

L'accesso ai dati trattati senza l'utilizzo di strumenti elettronici è consentito, come per i trattamenti di dati personali effettuati con mezzi elettronici, esclusivamente al personale espressamente incaricato.

Vi sono, inoltre, alcuni basilari comportamenti che, se messi in atto, riducono in maniera considerevole i rischi di accesso ai dati da parte di persone non autorizzate, di perdita di confidenzialità dei dati e della conseguente mancanza di disponibilità degli stessi.

In linea con ciò, risulta, ad esempio, assolutamente necessario raccogliere prontamente, nel caso di utilizzo di stampanti di rete o fax ubicati in locali comuni (per es. corridoi), i documenti stampati o ricevuti via fax, soprattutto se contenenti dati personali, in modo da preservarne la riservatezza del contenuto. È ugualmente rilevante, ai fini della tutela dei dati personali trattati nell'espletamento delle proprie mansioni, assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo dell'Ente, non siano lasciati a vista sulla scrivania ma conservati in cassetti o armadi. Conseguentemente e al fine di non eludere tali precauzioni, è opportuno conservare, con le dovute cautele, le chiavi utilizzate per i cassetti e gli armadi contenenti dati personali e sensibili/giudiziari. In particolare, è utile prevedere opportuni meccanismi per garantire, se necessario, ai propri colleghi la disponibilità delle stesse anche durante periodi di assenza dall'attività lavorativa (per es. copia delle chiavi depositate in segreteria, registro di presa in carico delle chiavi, ecc.).

Nei casi in cui atti o documenti contengano dati personali sensibili e/o giudiziari di rilevante importanza, si raccomanda di prevedere apposite procedure per la conservazione in archivi ad accesso selezionato, disciplinando le modalità di accesso a tali archivi in modo da consentire l'identificazione degli utenti che vi accedono. Conseguentemente, quando si prelevano tali atti o documenti dai suindicati archivi si sottolinea la necessità di controllare e custodire, fino alla restituzione, gli stessi, impedendo che ad essi possano accedere persone non autorizzate. In particolare, non lasciare incustoditi, neppure per brevi periodi, tali atti e documenti, provvedendo, eventualmente, a riporli in armadi o cassetti chiusi a chiave. In ogni caso, occorre restituire tali atti e documenti al termine delle operazioni di trattamento affidate, ricollocandoli negli archivi ad accesso riservato da cui sono stati prelevati.

13 RECUPERO DEI DATI DA PARTE DELL'ENTE IN ASSENZA DELL'UTENTE E INDICAZIONE DEL FIDUCIARIO

In questo paragrafo sono individuate apposite procedure volte a:

A. permettere all'Ente di recuperare dati, informazioni o documenti trattati nell'espletamento delle attività lavorative di un dipendente o un collaboratore, nei casi in cui l'assenza dello stesso sia programmata (ad esempio per ferie) oppure sia improvvisa e imprevista (ad esempio per malattia);
B. abilitare altri collaboratori (ad es. gli addetti ad una segreteria) all'utilizzo della casella di posta elettronica pur in presenza del titolare della casella stessa (ad es. il dirigente di struttura),

Tali procedure sono volte a bilanciare nel caso di cui alla lettera A), il diritto dell'Ente a garantire l'operatività organizzativa e amministrativa e l'uso consono degli strumenti forniti agli utenti con il diritto del lavoratore alla tutela della propria sfera di riservatezza anche nell'ambito della propria attività lavorativa.

È poi prevista una specifica procedura nel caso di cessazione del rapporto di lavoro (cfr. paragrafo 13.4).

Nel pieno rispetto del Provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" e degli orientamenti sia del Garante stesso sia giurisprudenziali in materia, con le procedure di seguito esplicitate sono disciplinati in maniera esaustiva i casi in cui i dati relativi

all'attività lavorativa del dipendente e del collaboratore regionale possano essere conosciuti dall'Ente nell'esercizio delle proprie prerogative organizzative. La priorità è concessa a modalità e strumenti che non comportano un accesso diretto ai dati personali e alle informazioni trattate dall'utente e quindi a funzionalità che meno comprimono il diritto alla riservatezza.

In accoglimento delle indicazioni ricevute dal Garante con il Provvedimento suindicato, figura centrale delle procedure di seguito specificate è il "fiduciario". Questi è un soggetto scelto liberamente da ciascun utente, che ha il compito di assicurare l'accesso ai dati trattati dall'utente fiduciante solo nei casi di assenza dello stesso. Quest'ultimo è ovviamente tenuto ad avvisare preventivamente il fiduciario e a comunicarne l'indicazione nominativa alla segreteria della Struttura di appartenenza, che ha l'onere di tenere aggiornato l'elenco dei fiduciari. A titolo esemplificativo il "fiduciario" potrebbe essere un collega che collabora nello stesso settore di attività lavorativa del fiduciante oppure che conosce o partecipa a un determinato progetto insieme al fiduciante stesso.

Il fiduciario, comunque, può accedere ai messaggi di posta oppure a files e cartelle del fiduciante soltanto nel caso in cui l'utente fiduciante stesso abbia, in caso di assenza programmata, attivato nei suoi confronti la funzione di delega ai messaggi della propria casella di posta elettronica oppure lo abbia autorizzato all'accesso a files e cartelle presenti nello spazio cloud personale.

Negli altri casi, qualora l'utente non abbia designato un proprio "fiduciario" e/o non abbia attivato alcuna funzione di delega all'accesso, la possibilità di accedere a suoi messaggi di posta oppure a files o cartelle presenti nello spazio cloud personale, può avvenire soltanto in casi di effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa. Soltanto in tale caso di emergenza sono previste e di seguito esplicitate le procedure che contemplano l'accesso alla casella di posta elettronica e ai dati dello spazio personale dell'utente su istanza del Responsabile della Struttura di appartenenza e per mezzo dei referenti informatici di Struttura.

È comunque fatto divieto allo stesso fiduciario o ad altro utente eventualmente delegato o autorizzato di accedere ai messaggi di posta elettronica e a file o cartelle che, già dall'oggetto e/o dalla denominazione e/o dalle proprietà, possano far prefigurare un contenuto riconducibile a informazioni personali non riconducibili ad attività lavorativa che, anche in tale sede, devono ricevere la dovuta tutela.

La nomina del fiduciario è strumento centrale e rilevante anche in ragione del fatto che l'Ente non utilizza risposte automatiche "Utente Fuori Sede" verso indirizzi di posta elettronica esterni, in quanto tale soluzione comporterebbe la segnalazione del dominio regionale di posta nelle Black List di Reputation: l'immediata conseguenza di ciò sarebbe il blocco della ricezione delle mail provenienti dall'Ente da parte dei sistemi di posta elettronica esterni.

È fatto divieto di conservare cartelle e documenti di lavoro sui dischi locali dei personal computer, dei portatili e di smartphone e tablet. Ciò comporterebbe, altrimenti, l'assunzione di rischi elevati in termini di confidenzialità, integrità e disponibilità dei contenuti prodotti da ciascun utente e, pertanto, deve essere limitata a operazioni su copie temporanee di lavoro.

Ogni utente ha a disposizione spazi di conservazione in cloud, eventualmente replicati e sincronizzati sul proprio dispositivo locale, ai fini di conservare documenti e bozze di lavoro; tale tecnologia garantisce backup, recupero di cancellazioni errate, gestione delle versioni e controlli di sicurezza.

Nei casi in cui l'Ente abbia necessità di accedere a contenuti necessari ad assicurare la continuità dell'attività lavorativa che l'utente abbia incautamente memorizzato sul disco locale della postazione di lavoro assegnata, si applicano per analogia le regole stabilite nei paragrafi seguenti.

13.1 RECUPERO DATI IN CASO DI ASSENZE PROGRAMMATE

In caso di assenze programmate (ad esempio in caso di ferie) e qualora vi siano esigenze di assicurare la continuità dell'attività lavorativa, l'utente condivide

- l'accesso in delega ai propri messaggi di posta elettronica a mezzo del software in utilizzo

- file o cartelle a mezzo del cloud

in favore del proprio fiduciario oppure in favore di altro soggetto, (ad es. quando lo stesso fiduciario è assente).

Il fiduciario o comunque il soggetto delegato farà accesso ai soli messaggi di posta elettronica o file/cartelle necessari ad assicurare la continuità dell'attività lavorativa.

Lo stesso "fiduciario" (o il delegato) può comunicare ai mittenti dei messaggi ricevuti nella casella di posta dell'utente assente, l'assenza dell'utente "fiduciante", e che, sino ad una determinata data, sarà lui stesso a prendere visione dei messaggi inviati su quella casella di posta.

13.2 RECUPERO DATI IN CASO DI ASSENZE NON PROGRAMMATE CON INDICAZIONE DEL FIDUCIARIO

In caso di assenze non programmate, come ad esempio per malattia, e qualora l'utente non abbia attivato le funzioni di condivisione descritte nel paragrafo precedente, il Responsabile della Struttura di appartenenza dell'utente assente, esclusivamente per effettiva e improrogabile necessità di assicurare continuità all'attività lavorativa, richiede al Responsabile del Servizio ICT Regionale per la Giunta regionale o al Responsabile del Servizio Funzionamento e Gestione per l'Assemblea legislativa, di attivare la funzione di delega all'accesso alla casella di posta elettronica o al cloud assegnato all'utente assente. La funzione di delega sarà attivata in favore dell'utente designato preventivamente quale "fiduciario" dall'utente assente.

L'istanza di accesso deve essere trasmessa anche in copia all'utente assente e al fiduciario dallo stesso nominato.

La funzione di delega su descritta rimane attiva per il tempo strettamente necessario al recupero dei contenuti e delle informazioni che si reputano indispensabili per dare continuità all'attività lavorativa dell'Ente oppure per un periodo di tempo limitato (quale ad esempio quello della malattia dell'utente assente) al termine del quale la funzione di delega è automaticamente disattivata.

Dopo aver effettuato l'accesso alla casella del collega "fiduciante" e dopo aver trasmesso al Responsabile di Struttura istante i messaggi di posta elettronica richiesti, di tali operazioni l'utente fiduciario redige verbale delle operazioni effettuate che consegnerà agli atti della struttura affinché anche l'utente stesso possa prenderne visione al rientro.

13.3 RECUPERO DATI IN CASO DI ASSENZE CON MANCATA INDICAZIONE DEL FIDUCIARIO

Qualora l'utente assente non avesse provveduto a individuare un proprio "fiduciario" e non avesse delegato neppure altri soggetti ad accedere ai propri contenuti, si prevede, sia nel caso in cui l'assenza sia programmata sia nel caso in cui non lo sia, che:

a) il Responsabile della Struttura di appartenenza dell'utente assente che esclusivamente per le succitate esigenze intende accedere a messaggi (inclusi gli eventuali allegati) presenti nella casella di posta elettronica o a file/cartelle presenti nel cloud assegnato allo stesso, deve effettuare la richiesta al Responsabile del Servizio ICT Regionale (per la Giunta regionale) o al Responsabile del Servizio Funzionamento e Gestione (per l'Assemblea legislativa);
b) l'accesso può essere autorizzato esclusivamente ai referenti informatici della Struttura di appartenenza dell'utente assente;
c) il referente ICT di struttura è designato incaricato del trattamento di dati personali che sia strettamente necessario effettuare al fine di adempiere ai compiti assegnatigli con l'istanza di cui alla lettera a);
d) il Responsabile del Servizio ICT Regionale dispone che uno degli amministratori di sistema attivi la funzione di delega sulla casella di posta o sul cloud dell'utente assente, a favore del referente ICT della Struttura di appartenenza dell'utente stesso;
e) è fatto divieto al referente ICT di accedere ai messaggi di posta elettronica o file/cartelle che, già dall'oggetto, possano far prefigurare un contenuto riconducibile a informazioni personali non relative all'attività lavorativa del soggetto assente;

f) la funzione di delega descritta rimane attiva per il tempo strettamente necessario al recupero dei contenuti che si reputano indispensabili per dare continuità all'attività lavorativa oppure per un periodo di tempo predeterminato (quale ad esempio quello della malattia dell'utente assente) al termine del quale la funzione viene automaticamente disattivata:
g) al termine della procedura di accesso e dopo aver trasmesso al Responsabile di Struttura istante i contenuti richiesti, il referente ICT di Struttura redige apposito verbale delle operazioni effettuate che consegnerà agli atti della struttura affinché anche l'utente stesso possa prenderne visione al rientro.

13.4 Reindirizzamento posta elettronica in caso di cessazione del rapporto di lavoro

Nei casi in cui l'utente cessi il proprio rapporto di lavoro con l'Ente, è concessa allo stesso la facoltà di reindirizzare per un periodo di tempo massimo di 30 giorni, i messaggi di posta elettronica ricevuti sulla casella di posta elettronica assegnata dall'Ente verso altro indirizzo email, previa autorizzazione del Responsabile della struttura di appartenenza. L'utente è tenuto ad indicare l'indirizzo di posta elettronica cui reindirizzare i messaggi di posta ricevuti.

Al fine di attivare questa funzione, l'utente deve effettuare istanza scritta al Servizio ICT regionale (per la Giunta, le agenzie e gli istituti regionali) o al Servizio Funzionamento e Gestione (per l'Assemblea legislativa).

13.5 Autorizzazione all'utilizzo della casella di posta elettronica ad altri collaboratori

Nel caso in cui un utente reputasse opportuno, al fine di organizzare in maniera più efficiente la propria attività lavorativa, autorizzare ulteriori collaboratori (esempio gli addetti alla Segreteria) all'utilizzo della propria casella di posta elettronica, calendario, attività, note, e contatti può utilizzare le funzioni di delega previste dall'applicativo di posta elettronica.

14 Ruoli e responsabilità

Al controllo del rispetto delle procedure, dei divieti e dei comportamenti degli utenti concorrono i seguenti ruoli e responsabilità:

Ruolo / Funzione	Responsabilità
Dirigente Responsabile della sicurezza	Adeguare i contenuti del disciplinare nel recepimento dell'evoluzione normativa e tecnologica.
Funzionario Responsabile della Posizione Organizzativa "Sicurezza informatica"	Responsabile della verifica del rispetto delle disposizioni contenute nel presente disciplinare, fatto salvo quanto di seguito specificato.
Funzionario Responsabile della Posizione Organizzativa "Governo dei sistemi di identità e piattaforme di Office Cloud Solutions ibride"	Responsabile delle procedure di accreditamento e del rilascio delle credenziali informatiche. Responsabile delle procedure di accesso ai fiduciari e delegati sui servizi di posta e dati in cloud.
Funzionario Responsabile delle funzioni di "Supporto agli utenti, gestione delle dotazioni e asset management ICT"	Responsabile della verifica del rispetto delle disposizioni contenute nel presente disciplinare con riferimento al corretto utilizzo dei posti di lavoro e delle dotazioni software personali.

Ruolo / Funzione	Responsabilità
Responsabili di struttura	Responsabile del riconoscimento “de visu” e della richiesta di accreditamento degli utenti esterni. Proroga e/o revoca dell’accreditamento ad un utente esterno. Approvazione della richiesta di assegnazione di nuove risorse del sistema informativo/informatico regionale ad un utente accreditato con le procedure di cui al paragrafo 4.5. Richiesta di revoca di risorse del sistema informativo/informatico regionale ad un utente accreditato. Diffusione e presa visione a tutti i propri collaboratori dei contenuti del presente documento. Valutazione della strumentazione da concedere in uso ad utenti esterni. Monitoraggio sul corretto utilizzo della stampa sicura.
Utenti	Rispetto delle disposizioni previste dal presente documento.
Personale del Servizio ICT Regionale	Effettuare un monitoraggio periodico della rete, dei dispositivi di sicurezza e delle postazioni di lavoro, al fine di individuare accessi non autorizzati ai dati, violazioni delle policy e compromissioni dei dispositivi. Tale monitoraggio viene effettuato senza alcuna comunicazione preventiva agli utenti, nell'interesse della tutela del patrimonio informativo dell'Amministrazione e della sicurezza delle informazioni degli utenti. Disporre procedure e/o soluzioni tecnologiche finalizzate a forzare il corretto rispetto da parte degli utenti delle disposizioni contenute nel presente disciplinare.

La violazione delle disposizioni contenute nel presente disciplinare, ferme restando eventuali responsabilità penali, civili o amministrativo-contabili, è rilevante sotto il profilo disciplinare e di responsabilità dirigenziale.

15 PUNTI DI CONTATTO ED INFORMAZIONI SUPPLEMENTARI

Per ulteriori informazioni sull’applicazione di questa policy utilizzare il seguente indirizzo email:

privacy@regione.emilia-romagna.it

securityadmin@regione.emilia-romagna.it

16 ISO27001: CONTROLLI APPLICABILI

L’Ente ha intrapreso un percorso di certificazione ISO27001 del Sistema di Gestione della Sicurezza delle informazioni. Al fine di ottenere e mantenere tale certificazione il Servizio ICT Regionale deve garantire il rispetto di determinati requisiti (definiti “Controlli”) contenuti nell’ANNEX A della norma ISO27001.

Di seguito quelli attinenti al presente documento:

Controllo A.6.2 della norma ISO 27001/2014: politica per dispositivi portatili e telelavoro.

Controllo A.8.3.1 della norma ISO 27001/2014: gestione dei supporti rimovibili.

Controllo A.9.1.2 della norma ISO 27001/2014: politica di controllo degli accessi.

Controllo A.9.2 della norma ISO 27001/2014: gestione degli accessi degli utenti.

Controllo A.9.3.1 della norma ISO 27001/2014: utilizzo delle informazioni segrete di autenticazione.

Controllo A.9.4 della norma ISO 27001/2014: controllo degli accessi ai sistemi e alle applicazioni.

Controllo A.11.1.2 della norma ISO 27001/2014: controllo di accesso fisico.

Controllo A.11.2.8 della norma ISO 27001/2014: apparecchiature incustodite degli utenti.

Controllo A.11.2.9 della norma ISO 27001/2014: politica di schermo e scrivania puliti.

Controllo A.12.2 della norma ISO 27001/2014: protezione dal malware.

Controllo A.12.4 della norma ISO 27001/2014: raccolta di log e monitoraggio.

17 GLOSSARIO

Termine/Acronimo	Descrizione
Analisi forense	insieme di tecniche rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova.
Autenticazione	l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente che accede ai sistemi informativi.
Black List di Reputation	Insieme di indirizzi (IP, mail) ai quali, sulla base dei comportamenti tenuti precedentemente (es. invio di spam), è impedito l'utilizzo di alcuni servizi informatici.
Cracking (strumenti di)	software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.
Dati giudiziari	i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
Dati personali	qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dati sensibili	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Identificazione informatica	la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.
Dispositivo mobile	sistema di elaborazione che può essere spostato e trasportato. Nel contesto del presente disciplinare tecnico, per dispositivo mobile si intende solo "smartphone" o "tablet", mentre negli altri casi si parla esplicitamente di "computer portatile", o "postazione di lavoro portatile"
Evidenza	nell'ambito dell'analisi forense, si intende una "traccia" di reato; la raccolta delle evidenze rappresenta una fase della gestione degli incidenti di sicurezza informatica, anche quando non siano presenti implicazioni legali.

Termine/Acronimo	Descrizione
Incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
Password	sequenza di caratteri alfanumerici che costituisce la chiave d'accesso ad un sistema protetto. In assenza di altri dispositivi, la password costituisce il meccanismo di sicurezza base per la protezione dell'accesso a risorse informatiche.
Patch	aggiornamento di un software per la correzione di un problema di sicurezza o di funzionalità.
Peer-to-peer (strumenti)	software che permettono l'utilizzo di una postazione di lavoro in modalità server per consentire lo scambio di file con altri utenti, anche esterni alla rete dell'Ente.
Phishing	tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).
Postazione di lavoro	Il pc o il portatile comprensivo di tutte le periferiche di input e output (mouse, tastiera, web cam, video, stampante collegata) che costituiscono la dotazione hardware assegnata ad un utente
Ransomware	tipo di malware che limita l'accesso del dispositivo che infetta (per esempio cifrando i dati), richiedendo un riscatto (*ransom* in Inglese) da pagare per rimuovere la limitazione
Responsabile	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
Scanning	attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.
Sniffing (strumenti di)	software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.
Spamming	l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.
Spyware	software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.
Supporto rimovibile	dispositivo su cui è possibile registrare dati che può essere facilmente rimosso dal sistema che lo legge/scrive, trasportato in altri luoghi e collegato ad altri sistemi. Esempi di supporti rimovibili sono: chiavette USB, hard disk esterni, CD ROM.
Titolare	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Worm	programma in grado di autodiffondersi sulla rete e verso altri sistemi.
Virus	programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.

REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Stefania Papili, Responsabile del SERVIZIO ICT REGIONALE esprime, ai sensi della deliberazione della Giunta Regionale n. 2416/2008 e s.m.i., parere di regolarità amministrativa in merito all'atto con numero di proposta DPG/2017/9145

IN FEDE

Stefania Papili