Ente di gestione delle aree protette dei Parchi Reali

Sede legale: *viale C. Emanuele II, 256 – 10078 Venaria Reale (TO) – tel. 011 4993328*
Sede operativa di Stupinigi: *viale Torino 4, (fraz. Stupinigi) – 10042 Nichelino (TO) – tel. 011 3587575*
partita IVA e codice fiscale 01699930010
http://www.parchireali.it – email: protocollo@parchireali.to.it – parchireali@legalmail.it

Disciplinare interno per l'utilizzo degli strumenti informatici 2023

Sommario

1. *INTRODUZIONE*

L'Ente di gestione delle aree protette dei Parchi Reali, di seguito denominato Ente, nell'espletamento della sua attività istituzionale opera prestando la massima attenzione alla sicurezza delle informazioni, perseguendo elevati livelli di sicurezza fisica e logica del proprio sistema informativo e adottando idonee misure organizzative, tecnologiche ed operative volte sia a prevenire il rischio di utilizzi impropri delle strumentazioni sia a proteggere le informazioni gestite nelle banche dati del sistema informativo.

Il presente documento definisce le regole e le condizioni per l'utilizzo degli **strumenti informatici dell'Ente** da parte dei dipendenti e di tutti coloro che, in virtù di un rapporto di lavoro a qualsiasi titolo (collaboratori, consulenti, stagisti, borsisti, fornitori, etc.), utilizzano strumenti informatici dell'Ente, nel seguito denominati Utenti.

Il presente disciplinare deve considerarsi integrato da tutte le procedure interne adottate nell'Ente, fra cui la procedura prevista in caso di violazione di dati personali pubblicata sul sito istituzionale dell'Ente (Piano di protezione e modello organizzativo a tutela dei dati personali), nell'apposita sezione Amministrazione trasparente» Disposizioni generali » Atti generali.

Il presente disciplinare è pubblicato sul sito istituzionale dell'Ente, nell'apposita sezione Amministrazione trasparente» Disposizioni generali » Atti generali.

Gli Utenti saranno preventivamente debitamente informati del contenuto del presente disciplinare.

1.1 Finalità del documento

Il presente documento definisce e detta agli Utenti specifiche regole e condizioni di utilizzo degli strumenti informatici aziendali attraverso:

- definizione di regole e procedure uniformi da applicarsi in tutte le aree organizzative;
- indicazione delle principali disposizioni normative in materia di utilizzo dei sistemi informativi e di protezione dei dati personali;
- definizione dell'ambito, delle modalità e dei limiti del monitoraggio e dei controlli attuabili dall'Ente nel rispetto della normativa vigente nonché delle regole e delle procedure interne;
- individuazione delle responsabilità degli Utenti in caso di inosservanza di regole e prescrizioni.

1.2 Contesto normativo

Il presente disciplinare è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8;
- D. Lgs. 196/2003 e s.m.i (Codice in materia di protezione dei dati personali);
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale);
- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza);
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento dell'EGAP Parchi Reali;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR);
- Piano dell'informatica dell'EGAP Parchi Reali;

2. *GLOSSARIO E DEFINIZIONI*

Ai fini del presente documento si intende per:

- **Amministratori di sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un sistema di elaborazione o di sue componenti o figure equiparabili, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, individuate dall'Ente in conformità al

Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009;

- **Applicazioni aziendali:** si considerano applicazioni aziendali:
  - Prodotti/programmi/App acquistati dall'amministrazione, di valenza generale o settoriale ed in quest'ultimo caso approvati dai sistemi informativi;
  - Applicazioni e servizio sviluppate ad hoc dai sistemi informativi, da terze parti ma sotto il coordinamento dei sistemi informativi ovvero da altre strutture con un processo di partecipazione e approvazione da parte dei sistemi informativi e che seguono le regole di gestione previste nei casi precedenti;
  - Applicazioni esterne che l'amministrazione utilizza secondo le regole di gestione e di sicurezza delle medesime a titolo di mero esempio possono essere la piattaforma mepa, abbonamenti a servizi informativi, portale ANAC, etc.
- **Dispositivi mobili:** apparecchi di telecomunicazione portatili (tablet, smartphone, etc.);
- **File di log:** registrazioni sequenziali e cronologiche delle operazioni effettuate da un sistema informativo, necessarie per la risoluzione di problemi ed errori; tali operazioni possono essere effettuate da un Utente oppure avvenire in modo totalmente automatizzato;
- **Pila software:** elenco di software installati o installabili sui dispositivi aziendali dell'Ente;
- **Postazione di lavoro (PdL):** personal computer (desktop o portatile) messo a disposizione dall'Ente a ciascun Utente per l'espletamento dell'attività lavorativa;
- **Strumenti informatici:** personal computer fissi o portatili, stampanti locali o di rete, programmi e prodotti software, apparecchiature adoperate per la comunicazione unificata (videoconferenza, telefonia fissa e mobile, chat, messaggistica generica, social network, posta elettronica, condivisioni, accessi remoti, etc);
- **Utenti:** personale dipendente, personale comandato da altre pubbliche amministrazioni, collaboratori, consulenti, tirocinanti, stagisti, fornitori esterni e coloro che, in virtù di un rapporto contrattuale in essere a qualsiasi titolo con l'Ente, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione dall'Ente;
- **Spazi di condivisione:** le cartelle condivise nella rete locale o sui cloud dell'Ente per la memorizzazione di informazioni in formato digitale a scopo esclusivamente lavorativo;
- **PEC:** è un sistema di comunicazione quale la posta elettronica ordinaria, a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere ai messaggi un valore legale equiparato alla Posta Raccomandata con ricevuta di ritorno (A/R). Il valore legale è assicurato dai gestori del servizio PEC del mittente e del destinatario, per le sole comunicazioni inviate da una casella PEC e ricevute da un'altra casella PEC, che certificano:
  - data e ora dell'invio del messaggio da parte del mittente;
  - data e ora dell'avvenuta consegna del messaggio al destinatario;
  - integrità del messaggio (ed eventuali allegati) nella trasmissione da mittente a destinatario;
  - le caselle PEC dell'Ente sono, di norma, integrate nel sistema di protocollo informatico.
- **Sistema informatico dell'Ente:** l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, personal computer, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Ente;
- **Centro Elaborazione Dati CED:** funzione organizzativa, afferente all'area Servizi Generali, che ha il compito di coordinare e mantenere il Sistema informatico dell'Ente.

3. PRINCIPI GENERALI

Gli strumenti informatici sono assegnati agli Utenti per lo svolgimento dell'attività lavorativa e devono essere utilizzati con modalità e mediante comportamenti adeguati ai compiti assegnati e alle responsabilità connesse, nel rispetto del Codice di comportamento dei dipendenti della pubblica amministrazione e delle normative e direttive interne.

Nell'esecuzione della propria attività lavorativa, gli Utenti sono tenuti ad attenersi alle seguenti istruzioni generali:

a) effettuare la propria attività uniformandosi alle disposizioni dell'Ente e alle istruzioni ricevute;
b) custodire con diligenza gli strumenti informatici loro affidati, segnalando tempestivamente alle strutture preposte, secondo le modalità previste, ogni danneggiamento, smarrimento o furto;
c) mantenere la riservatezza sulle informazioni e sui dati personali di cui siano venuti a conoscenza durante lo svolgimento della propria attività;

d) in caso di cessazione dal servizio o dalla prestazione svolta per l'Ente, astenersi dalla diffusione di informazioni, dati e documenti acquisiti durante lo svolgimento della propria attività;
e) adottare ogni misura di sicurezza idonea a scongiurare rischi di perdita o distruzione (anche accidentale) dei dati;
f) garantire la corretta custodia di atti e documenti adottati dall'Ente

I rapporti e i comportamenti, a tutti i livelli organizzativi, sono improntati ai principi di onestà, correttezza, trasparenza, riservatezza, imparzialità, diligenza, lealtà e reciproco rispetto.

I trattamenti dei dati personali effettuati durante l'accesso alla Rete e l'utilizzo del Sistema Informatico dell'Ente, devono inoltre rispettare quanto previsto dalle normative vigenti in materia di protezione dei dati e svolgersi nell'osservanza dei seguenti principi cogenti:

- **il principio di necessità,** secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (artt. 5 e 6 del GDPR). Deve essere quindi garantito, per impostazione predefinita, che siano trattati solo i dati personali necessari per ciascuna finalità del trattamento (obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi (Privacy by default art. 25, comma 2 del GDPR).
- i principi di **correttezza e trasparenza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 12 del GDPR). Le tecnologie dell'informazione (in modo più marcato rispetto alle apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa; ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati. I dati personali saranno trattati quindi in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5 del GDPR) nel rispetto degli obblighi di cooperazione con l'autorità di controllo quando questa ne faccia richiesta (art. 31 del GDPR).
- i trattamenti di dati personali devono essere effettuati per finalità determinate, esplicite e legittime, osservando **il principio di pertinenza** e non eccedenza, ovvero di limitazione delle finalità e minimizzazione dei dati (art. 5, comma 1 lett. b) e c) del GDPR). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere 8 giugno 2017 del EDPB2 in merito al trattamento dei dati personali dei lavoratori, che ha integrato quanto già previsto in passato con il Parere n. 8/20013 ed il "Documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sul luogo di lavoro" del 2002 del Garante per la protezione dei dati personali sul trattamento di dati personali nell'ambito dei rapporti di lavoro. I dati devono quindi essere: adeguati, pertinenti, esatti ed aggiornati, oltre che limitati a quanto necessario rispetto alle finalità (art. 5 del GDPR), e comunque da trattare in modo da garantirne **un'adeguata sicurezza** (artt. 24 e 32 del GDPR). Quando la violazione della sicurezza dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il datore di lavoro deve darne notizia all'interessato senza ingiustificato ritardo (art. 34 del GDPR).
- il datore di lavoro deve distinguere i casi in cui per eseguire un trattamento di dati personali è richiesto il (previo) **consenso** dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il datore di lavoro deve essere in grado di dimostrare che il consenso è stato effettivamente prestato (artt. 6 e 7 del GDPR). Per quanto riguarda l'informativa invece, il datore di lavoro deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo (artt. 13 e 14 del GDPR).
- il datore di lavoro, per procedere al trattamento dei dati personali, deve rispettare il diritto dell'Interessato a non essere sottoposto ad una decisione basata unicamente su un **trattamento automatizzato** dei dati che produca effetti che incidano significativamente sulla sua persona (art. 22 del GDPR); deve inoltre rispettare **i diritti degli interessati** in termini di accesso, rettifica, cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto di opposizione al trattamento (ove il datore di lavoro non dimostri l'esistenza di motivi legittimi cogenti), con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul datore di lavoro (artt. 15-21 del GDPR).

In relazione alla tutela del diritto d'autore e all'utilizzo del software e dei prodotti informatici, devono essere rispettate tutte le misure atte ad assicurare un utilizzo delle risorse conforme alle disposizioni normative che tutelano il copyright, i brevetti e la proprietà intellettuale, ai sensi della Legge 22 aprile 1941 n.633 e s.m.i.4. Pertanto, tutti gli Operatori e Utenti che usufruiscono del Sistema Informatico dell'Ente devono utilizzare il software installato sulla postazione lavorativa (PC o dispositivi mobili) o disponibile attraverso la rete LAN, nel rispetto dei termini contrattuali e/o delle licenze in concessione d'uso, osservandone

attentamente le limitazioni relative, ad esempio, al numero di copie riproducibili, al numero di utenti fruitori ed alle scadenze temporali delle concessioni.

4. REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI

4.1 Credenziali di autenticazione al dominio

Gli Utenti possono accedere al Sistema informatico dell'Ente esclusivamente per lo svolgimento delle mansioni lavorative/incarichi ad essi affidati, in forza di un contratto o altro accordo in essere con l'Ente, ed esclusivamente per scopi leciti.

Gli Utenti possono accedere al Sistema Informatico dell'Ente solo previa autorizzazione del Direttore dell'Ente, tramite credenziali di autenticazione (es. username e password) o altri metodi di autenticazione "forte", quali la Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE) e SPID.

GliUtenti si impegnano ad evitare pratiche che possono esporre l'Ente a rischi informatici (es. possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche di proprietà dell'Ente).
Laddove tali pratiche non siano evitabili, gli Utenti si impegnano ad adottare comportamenti tesi a minimizzare tali rischi.

Gli Utenti sono tenuti a segnalare presunte o accertate violazioni alla sicurezza delle risorse informatiche dell'Ente, al Direttore dell'Ente o persona da lui delegata e per conoscenza al Responsabile della Sicurezza delle Informazioni e al Responsabile dell'Ufficio.

Gli strumenti adottati per l'accesso Sistema informatico dell'Ente, sono di uso strettamente personale e pertanto gli Utenti sono tenuti a custodirli in modo appropriato, al fine di garantirne la riservatezza e l'integrità.

L'accesso alle applicazioni del sistema informativo dell'Ente avviene attraverso autenticazione mediante credenziali di dominio.

Le credenziali di autenticazione, da gestire nel rispetto delle regole stabilite, sono strettamente personali e non devono essere comunicate né rese disponibili ad altri soggetti.

In caso di diffusione accidentale, anche solo presunta, le password devono essere immediatamente modificate e l'incidente va immediatamente segnalato.

Il sistema di controllo degli accessi presente nell'Ente implementa le seguenti regole:

- nell'ambito delle credenziali di accesso, la *username* attribuita dall'Amministratore di Sistema è immodificabile;
- composizione di password complesse, che abbiano una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
- all'atto del primo accesso al Sistema informatico dell'Ente (login), con le credenziali di autenticazione, l'Operatore o l'eventuale Utente così come definito alla let. x) dell'Art. 3,deve obbligatoriamente modificare la password comunicatagli dall'Amminsitratore di sistema con una nuova password personale, che dovrà mantenere segreta e custodire con la massima diligenza;
- impossibilità di riuso delle ultime password utilizzate;
- l'Utente è considerato l'unico responsabile delle attività espletate tramite la propria username, la propria CNS, la propria CIE e le proprie credenziali SPID; vige a tal fine una presunzione di corrispondenza tra Utente e username e, laddove applicabile, la CNS, la CIE o SPID;
- reinizializzazione (reset) della password e riattivazione delle utenze disabilitate, secondo le procedure in vigore.

I dettagli dei requisiti richiesti sull'utilizzo delle password sono riportati nell'allegato **Password.**

4.2 Utilizzo di applicazioni aziendali

L'accesso alle applicazioni e il loro utilizzo devono avvenire secondo le regole dettate dal presente Disciplinare, con riferimento ai diversi ruoli di responsabilità specificamente individuati nell'Ente per le varie tipologie di utenza.

All'atto della cessazione/interruzione del rapporto di lavoro o dell'attività lavorativa svolta a qualsiasi titolo per conto dell'Ente, ferma restando la disabilitazione all'uso degli applicativi e delle funzionalità da parte del servizio a cui afferisce il CED, è fatto obbligo di restituzione delle strumentazioni elettroniche (pc portatili, tablet, cellulari ecc.) già affidate per l'esplicazione delle funzioni connesse al rapporto di lavoro.

4.3 Postazione di lavoro

Le postazioni di lavoro (PdL) sono gestite dall'Ente che le assegna agli Utenti. È vietato qualsiasi utilizzo che deturpi o rovini la PdL e tutti gli accessori/periferiche in assegnazione.

La postazione di lavoro è provvista di:

- sistema operativo e sue estensioni: antivirus, programmi di office automation (programmi per la redazione di documenti, di fogli elettronici, di gestori di database);
- eventuali software specifici correlati alle necessità delle attività lavorative.

L'assegnatario della PdL è profilato come utente con diritti amministrativi limitati a livello locale, con obbligo di non apportare alcuna modifica senza preventiva autorizzazione dell'Amministratore di Sistema dell'Ente.

L'Utente assegnatario della postazione di lavoro è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole:

a) la PdL è assegnata all'Utente per lo svolgimento della propria attività lavorativa;
b) la PdL non deve essere accessibile a soggetti non autorizzati;
c) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa sugli spazi assegnati;
d) ogni Utente deve tenere comportamenti tali da ridurre al minimo il rischio di attacco al Sistema informatico dell'Ente attuati mediante virus o altro software aggressivo;
e) nel caso di malfunzionamenti o avvisi sospetti, ogni Utente è tenuto a comunicarli all'Amministratore di sistema;
f) durante l'allontanamento dalla PdL, l'Utente deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password;
g) al termine della giornata lavorativa, soprattutto per motivi di sicurezza, deve essere effettuato lo spegnimento delle PdL;
h) obbligo di formazione e aggiornamento in ambito informatico-digitale, secondo quanto indicato e messo a disposizione dall'Ente in riferimento al ruolo e professionalità.

4.4 Postazione di lavoro portatile

Per quanto riguarda la postazione portatile, valgono tutte le regole già descritte per le postazioni fisse.

Le postazioni portatili devono essere detenute presso la sede aziendale durante l'espletamento del'attività lavorativa "in sede" all'assegnatario, salvo autorizzazione esplicita del Direttore dell'Ente di utilizzo al di fuori della sede dell'Ente.

Si evidenzia che le stazioni di lavoro portatili, utilizzate al di fuori della sede dell'Ente, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute.

L' Utente è responsabile del PC portatile e/o accessori (macchina fotografica, videoproiettore) a lui temporaneamente assegnati e deve custodirli con cura e diligenza, sia all'interno degli uffici dell'Ente, sia durante gli spostamenti esterni, fino alla loro riconsegna.

Particolare attenzione deve essere prestata:

a) nella connessione a reti telematiche esterne;
b) nella cancellazione sicura di eventuali file e dati personali memorizzati nel medesimo, prima della riconsegna.

Le postazioni di lavoro portatili devono essere verificate dagli addetti al CED per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. La verifica avviene mediante appuntamento concordato con tali addetti. In caso di significativo rischio di compromissione o/e sicurezza, tale Servizio può richiedere all'Utente lo spegnimento della PdL portatile fino a tale verifica ovvero bloccare il dispositivo da remoto.

4.5 Smartphone e SIM

La concessione dello smarthphone aziendale e della SIM card sono autorizzate dal Direttore dell'Ente su formale e motivata richiesta da parte del Responsabile Area/Settore o Responsabile dell'Ufficio, per il personale di propria competenza.

L'Utente è responsabile dell'utilizzo del dispositivo assegnato ed esssendo strumento di lavoro si ha obbligo di rispetto delle seguenti regole:

a) uso per lo svolgimento dell'attività lavorativa;
b) divieto di utilizzo da parte di soggetti non autorizzati;
c) immissione di un codice per lo sblocco dello schermo;
d) diligente uso e conservazione dello smarthphone e dei dati e utenza messi a disposizione dall'Ente;
e) nel caso di malfunzionamenti o avvisi sospetti, ogni Utente è tenuto a comunicarli al proprio Responsabile e all'ufficio dell'Ente competente per il relativo acquisto o sostituzione;
f) in caso di furti o smarrimenti ogni Utente è tenuto a comunicarli al proprio Responsabile e all'ufficio dell'Ente competente per il relativo acquisto o sostituizione, ai fini dell'immediato blocco dell'utenza e relative denunce alle autorità competenti;
g) gli Utenti, affinchè possano essere immediatamente rintracciabili nei casi di necessità, hanno l'obbligo di mantenere il dispositivo in funzione durante tutto l'orario di lavoro e di reperibilità ove prevista;
h) per l'utilizzo delle Istant Messanger si richiamano le regole del punto 4.8;
i) per la navigazione in internet si richiamano le regole del punto 4.9;

È prevista la possibilità di assegnazione di SIM dati, indipendentemente dal telefono cellulare aziendale, per i servizi che ne dovessero fare richiesta per motivi collegati alle attività istituzionali proprie (es. monitoraggio di parametri ambientali, controllo remoto di apparecchiature, trasmissione di dati tra sistemi, comunicazione machine-tomachine, etc.).

In caso di cessazione del rapporto di lavoro lo smarthphone e le SIM aziendali dovranno essere riconsegnate all'Ente.

4.6 Altri dispositivi

Con riferimento ad altri dispositivi assegnati ai dipendenti, quali stampanti, fotocopiatrici, scanner, tablet valgono le medesime regole comportamentali adottate per le PdL.

4.7 Software a corredo

La lista software utilizzabili nell'Ente è contenuta nel documento allegato **Pila Software** e riguarda tutti i dispositivi aziendali.

L'eventuale utilizzo di software di tipo portable (che non richiedono installazione) o installabili con i permessi dell'Utente è nella completa responsabilità dell'Utente, sia per gli aspetti di diritto di proprietà intellettuale sia per quelli di sicurezza.

In relazione alla strategia Cloud della PA, nata per favorire l'adozione del modello del Cloud computing nelle pubbliche amministrazioni italiane e in linea con le indicazioni della Strategia per la Crescita digitale e con le previsioni del Piano Triennale per l'Informatica, nella scelta del software l'Utente deve dare precendeza alla versione Cloud e a fornitori già inseriti nel registro Agid dei software qualificati per il cloud della PA, in quanto già sottoposti alla valutazione dei requisiti di Cyber Security necessari per operare con la PA. Nel caso il fornitore non sia presente nel registro Agid,di seguito sono elencati i principali aspetti da valutare nella scelta:

- **Governance:** include gli aspetti utili a valutare la "maturità" del cloud provider in tema di Cyber Security. Fanno parte di questa categoria: policy, framework di Cyber Security Management System, processi per la gestione dei rischi di sicurezza, sia interni sia legati alla catena dei sub-fornitori, selezione, sensibilizzazione e formazione del personale;
- **Compliance:** consente di valutare la capacità del provider di soddisfare i requisiti di conformità a leggi, regolamenti e standard di riferimento per l'Ente. Include tipicamente la conformità alle normative privacy (ad esempio, il GDPR),

l'ubicazione geografica dei data center e di conseguenza dei dati, eventuali coperture assicurative nel caso di data breach e la disponibilità a fornire evidenze di conformità a standard e regolamenti;

- **Business Continuity:** consente di valutare la capacità del provider di garantire la continuità dei servizi offerti e la disponibilità delle operazioni e dei dati. Include aspetti quali la disponibilità di procedure e di soluzioni tecniche (facility, sistemi, reti, backup ecc., fino alla disponibilità di siti di disaster recovery) atte a coprire scenari di crisi di diversa natura e portata, dal guasto limitato al disastro esteso, dovuti sia a eventi naturali che ad azioni deliberate o errori;
- **Infrastructure Security:** include le misure di sicurezza fisica e ambientale (dal controllo degli accessi fisici a impianti anti-incendio e allagamento), di sicurezza delle reti (segmentazione, sicurezza perimetrale, accessi remoti sicuri, IDS/IPS ecc.) e delle architetture di virtualizzazione (ad esempio, multi tenancy per segregare i dati di clienti diversi);
- **Identity & Access Management:** fanno parte di questa categoria le misure per il controllo degli accessi logici a sistemi, apparati, servizi e applicazioni, sia da parte del personale del provider per finalità di gestione sia da parte degli utenti dei clienti per accedere a servizi e dati. Include soluzioni di user e password management, strong authentication, nonché la capacità di integrazione con i sistemi di user management dei clienti;
- **Data Protection:** consente di valutare la capacità del provider di proteggere i dati dei clienti da accessi e modifiche non autorizzate. Include la crittografia sia dei dati memorizzati "at rest" sia di quelli in transito (ad esempio a/da i sistemi dei clienti), le procedure di gestione delle chiavi crittografiche (key management), le soluzioni/procedure di backup e restore e la gestione/restituzione dei dati alla cessazione dei contratti;
- **Host, Middleware & Application Security:** include le misure per la sicurezza dei server fisici, quali antivirus, hardening e patching, del middleware (quali API security, database security) e delle applicazioni (adozione di best practice di sviluppo di codice sicuro, web application firewall -WAF, code inspecting ecc.);
- **Operation & Monitoring:** include procedure di patch management, interventi di vulnerability assessment, il tracciamento, il monitoraggio dei log, strumenti e procedure per la gestione e la notifica degli incidenti di sicurezza.

4.8 App Istant Messanger

L'utilizzo delle App di Istant Messanger (es. WhatsApp) come strumento di lavoro è obbligatorio, nell'ambito e orari di lavoro, per i possessori di smarthphone e SIM aziendale.

Salvo ragioni di forza maggiore, l'Utente ha l'obbligo di mantenere attive e consultare almeno una volta, le chat aziendali durante l'orario di lavoro.

L'Utente ha inoltre l'obbligo di mantenere attiva sull'App di Istant Messanger l'opzione delle spunte di avvenuta ricezione del messaggio e della sua lettura (es. WhatsApp: 1 spunta messaggio inviato, due spunte messaggio ricevuto, due spunte blu conferma della lettura).

Le chat aziendali, sotto il controllo degli Amministratori del gruppo, debbono limitarsi a trattare argomenti attinenti all'attività lavorativa o comunque a questa connesse.

4.9 Social Media: profili aziendali

Per "Social Media: profili aziendali" si intende qualsiasi strumento di comunicazione online che permette la creazione, pubblicazione e lo scambio pubblico di contenuti generati per conto dell'Ente. I Social Media includono quindi sia i social network, sia i blog e le piattaforme di microblogging tra cui per es. Twitter, Facebook, Myspace, YouTube, Flickr, LinkedIn, Instagram, Pinterest, Google+ e Tumblr.

I Social Media rivestono un ruolo importante nella creazione di un rapporto di fiducia e "reputazione" nei confronti dei follower dei profili aziendali dell'Ente.

Gli Utenti con mansioni di Amministratore dei profili aziendali dell'Ente sono obbligati a:

a) concordare con l'Ente un adeguato processo di approvazione dei contenuti da pubblicare;
b) conservare con cura e non cedere a Terzi non autorizzati le credenziali di accesso ai profili aziendali;

c) monitorare la reputazione dell'Ente sui Social Media e comunicare con sollecitudine ai vertici dell'ente eventuali contenuti inappropriati o diffamatori postati, provvedendo celermente (ove possibile e ove ritenuto opportuno) alla relativa eliminazione;
d) non diffondere dati ed informazioni sensibili o riservate e materiale coperto da diritti di proprietà intellettuale (incluso il copyright);

È bene ricordare che anche i contenuti condivisi su account personali, una volta messi in rete, possono avere risonanza globale. Gli Utenti dotati di profili personali sui Social Media (es. blog, social network) o di un sito web personale in cui è menzionato l'Ente o in cui si può essere identificati come dipendenti e/o collaboratori di esso da parte di terzi, sono tenuti:

a) a comunicare ai lettori che i pareri espressi sono personali;
b) a non diffondere dati e informazioni sensibili e riservati riguardanti la propria attività lavorativa con l'Ente (es. la corrispondenza interna; informazioni di terze parti di cui è a conoscenza - ad esempio partner, istituzioni, utenti, stakeholder, ecc. - o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici; decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati e pubblicati o diffusi dall'Ente);
c) rispettare la privacy degli altri Utenti, evitando riferimenti all'attività lavorativa svolta, fatte salve le informazioni di dominio pubblico.

4.10 Navigazione in Internet

La navigazione in internet è messa a disposizione del personale come fonte di informazione per le finalità di documentazione, ricerca e studio, utili per lo svolgimento della prestazione lavorativa.
Qualsiasi operazione effettuata sulla rete esterna (accesso a siti web per necessità non inerenti l'attività lavorativa, salvataggio di file, partecipazione a forum, etc.) è posta sotto la responsabilità dell'Utente, che deve mantenere un comportamento lecito e tale da non compromettere le attività e il buon nome dell'Ente.

Ogni Utente è tenuto a osservare le seguenti regole comportamentali:

- utilizzare internet per fini leciti, astenendosi da qualsiasi comportamento che possa avere natura oltraggiosa e/o discriminatoria verso terzi;
- non effettuare il download o lo scambio peer-to-peer di materiale audiovisivo, fotografico,software ed in genere di ogni altra tipologia di materiale digitale non legati ad un uso d'ufficio e che possa sottintendere presunte o palesi violazioni del copyright in ambito nazionale ed internazionale;
- trasferire sul proprio dispositivo (download) solo file da siti web verificati e affidabili, tenendo presente che quando si trasferisce materiale da internet occorre prestare la massima attenzione al fine di non incorrere in violazioni di diritti di proprietà intellettuale;
- non utilizzare social network, forum, chat e simili per scambiare informazioni riservate o lesive dell'immagine dell'Ente e dei colleghi;
- la navigazione in internet avviene in modalità trasparente e non anonima, soprattutto se attraverso intranet o strumenti aziendali; in ogni caso è vietato accedere a siti i cui contenuti non siano adeguati all'immagine e al buon nome dell'Ente;
- si rammenta che, limitatamente alle finalità indicate nelle specifiche Informative sulla protezione dei dati personali predisposte dall'Ente ai sensi degli artt.13 e 14 del GDPR, i sistemi di accesso ad Internet dell'Ente tengono traccia della navigazione degli Operatori;
- ogni Operatore è obbligato ad utilizzare il servizio di accesso al web, ponendo la massima attenzione alla sicurezza del Sistema informatico e telematico dell'Ente e nel rispetto di quanto previsto dal Codice di Comportamento dei dipendenti dell'Ente.

Al fine di prevenire l'accesso a siti web e risorse internet potenzialmente nocivi, per la navigazione dalla rete aziendale l'Ente adotta soluzioni di sicurezza basate su filtri e decriptazione delle informazioni della navigazione Internet attraverso i quali l'accesso a specifiche e determinate categorie di siti è bloccato a priori; i tentativi di accesso a tali siti (ad esempio siti malevoli, gioco d'azzardo) vengono bloccati e all'Utente è inviato un avviso in cui viene spiegato il motivo del blocco. Al fine di prevenire il download di file o pagine web contenenti codici malevoli, l'Ente adotta soluzioni di sicurezza basate su tecnologie antimalware che

effettuano la scansione dei contenuti della navigazione Internet e bloccano il download del contenuto in caso di rilevazione di codice malevolo.

4.11 Posta elettronica e PEC

Tutti gli Utenti sono dotati di una casella di posta elettronica sul dominio dell'Ente. Le caselle devono essere utilizzate per l'esercizio della propria attività lavorativa.

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni, come indicato nell'allegato **Utilizzo della posta elettronica da parte degli Utenti**.

Il sistema di posta elettronica prevede:

- la possibilità di imporre limiti all'utilizzo del servizio, ad esempio sul numero dei destinatari di un messaggio, sulla dimensione degli allegati che sarà possibile inviare e/o sulla dimensione complessiva della casella di posta elettronica;
- per le e-mail inviate a destinatari esterni al dominio di posta elettronica dell'Ente, è predisposto un avvertimento (disclaimer) inserito automaticamente in calce al messaggio. In tale disclaimer viene dichiarata la natura riservata del contenuto ed è inserito un invito alla cancellazione per chi non fosse il destinatario previsto. Non è consentito inserire disclaimer personalizzati in calce alla comunicazione;
- una scansione di sicurezza automatica dei messaggi , al fine di prevenire la diffusione di e-mail contenenti malware e/o phishing; a fronte di tale controllo si potrebbe rendere necessario l'accesso, da parte dell'amministratore di sistema, ai singoli messaggi identificati come potenzialmente malevoli, su richiesta dell'Utente e in affiancamento allo stesso;
- un sistema automatico di classificazione dei messaggi ricevuti (spam o posta indesiderata), in cui confluiscono tutti i messaggi non reputati leciti dall'algoritmo anti-spamming.

L'Utente è riconosciuto quale unico autore dei messaggi inviati dalla sua casella di posta elettronica personale fornitagli dall'Ente ed è considerato, inoltre, unico responsabile dell'attività espletata tramite la propria casella di posta personale.

Nell'utilizzo del servizio l'Utente ha l'obbligo di:

- implementare, sulla propria postazione di accesso alla posta elettronica tutte le misure indicate dall'Ente o di normale diligenza atte ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili e garantire la funzionalità della stessa casella;
- salvo ragioni di forza maggiore, consultare la casella di posta elettronica almeno una volta durante la giornata lavorativa;
- non usare la posta elettronica per motivi non inerenti al rapporto di lavoro in essere con l'Ente;
- in accordo con il Responsabile dell'Area/Settore o Responsabile dell'Ufficio, attuare tutte quelle misure di carattere organizzativo procedimentale tese ad evitare l'uso della casella di posta elettronica come sistema documentale, privilegiando altresì gli strumenti istituzionali all'uopo preposti (e.g. protocollo informatico, cartelle condivise, cloud);
- utilizzare il servizio di posta elettronica nel rispetto della legge e del presente Disciplinare, ponendo la massima attenzione alla sicurezza del Sistema informatico e telematico dell'Ente;
- inserire la propria firma utilizzando il format definito dall'Ente per l'invio di messaggi verso l'esterno, uniformando la firma automatica in calce all'email;
- proteggere la privacy dell'interlocutore evitando, qualora non necessario, di inoltrare messaggi altrui senza il previo consenso dell'interessato;
- inviare le e-mail esclusivamente a nome proprio. Si ricorda che è considerato mittente il proprietario della casella da cui è inviata l'e-mail, anche in presenza di altri nominativi;
- evitare l'invio, tramite le caselle di posta elettronica, di messaggi ingiuriosi, minatori, lesivi dell'immagine dell'Ente o che utilizzino linguaggi o immagini oscene, ingannevoli o diffamatorie;
- evitare di creare o rispondere a "catene di Sant'Antonio", appelli o richieste non pertinenti all'attività lavorativa dell'Ente;
- evitare l'invio o l'inoltro di messaggi estranei al contesto lavorativo a un gran numero di indirizzi o a liste di distribuzione interne all'Ente;

- evitare l'utilizzo dell'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
- evitare di diffondere, all'esterno dell'Ente, indirizzi di posta elettronica di altri colleghi, per motivi non legati all'attività lavorativa;
- comunicare all'Amministratore di sistema qualsiasi malfunzionamento del proprio indirizzo di posta elettronica;
- evitare invii multipli di e-mail senza mascherare gli indirizzi delle caselle email dei vari destinatari (ccn:), se non strettamente necessario;
- evitare di sovraccaricare il sistema con l'invio di allegati di dimensioni elevate ed evitare immagini (es. sfondi) o grafismi superflui;
- evitare di effettuare comunicazioni esterne così contenenti categorie particolari di dati personali o dati personali relativi a condanne penali e reati sensi del GDPR, nonché documenti dell'Ente per i quali l'accesso è regolato dalla Legge n. 241/199016, in modo particolare se riservati o protetti dal diritto d'autore17;
- in caso di assenza dell'Utente, temporanea o protatta nel tempo, di attivare la funzione di risposta automatica con l'indicazione al mittente del periodo di assenza e dei riferimenti alternativi dell'Ente a cui potersi rivolgere.

L'Utente è responsabile dell'efficace organizzazione e gestione della propria casella di posta elettronica, attuando buone pratiche, quali a titolo esemplificativo e non esaustivo:

a) cancellare i documenti inutili e/o che possono essere reperiti su altri sistemi istituzionali;
b) evitare di richiedere l'invio di allegati ingombranti, privilegiando modalità alternative di invio meno invasive (es. permalink, link a cartelle condivise);
c) organizzare le e-mail in cartelle per mittente/argomento, ai fini di una successiva ricerca.

Ciascun Responsabile dell'Area/Settore o Responsabile dell'Ufficio può richiedere l'attivazione di una **casella di posta elettronica Certificata PEC**, previa autorizzazione del Direttore dell'Ente, indicando le modalità di costante consultazione dei messaggi in arrivo.

Nel caso in cui l'Utente non presti più la sua attività lavorativa presso l'Ente, la casella di posta elettronica sarà prontamente disattivata cancellandone il contenuto, su richiesta via PEC al gestore del provider di posta elettrica a cui l'Ente ha affidato il servizio.

Il backup della casella di posta sarà conservato dall'Amministratore di Sistema presso l'Ente per n.6 mesi prima della sua definitiva cancellazione.

Si consiglia nella disattivazione di caselle di posta di Area/Servizio (non nominative), l'indicazione di un Alias (indirizzo mail alternativo di inoltro).

L'elenco delle caselle di posta elettronica certificata è pubblicato sul sito internet dell'Ente in "Amministrazione trasparente» Organizzazione » Telefono e posta elettronica.

4.12 Spazi di condivisione file server: on premise o cloud

Gli spazi di condivisione file server (on premise) o cloud, devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo (es. non salvare né su cloud, né su spazi di rete aziendale, né su Pdl file coperti da copyright come film, musica e foto personali). I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali, a seguito di guasti alle PdL.

Sulle unità di rete condivise vengono svolte regolari attività di controllo, amministrazione e back up da parte del CED.

Lo spazio disco messo a disposizione ha dei costi notevoli sia in termini economici che di tempo dedicato alla manutenzione, pertanto ogni utente periodicamente deve provvedere alla cancellazione dei file obsoleti o inutili.

Per permettere la corretta sincronizzazione del proprio profilo è buona prassi:

- svuotare periodicamente la cartella di download ed il cestino. Per chi lavora su più postazioni condivise la cartella di dowload deve essere svuotata non solo su una postazione ma su tutte quelle su cui ci si collega;
- non salvare e intasare il desktop di file e non salvare documenti direttamente sul PC (es.C: e desktop: non sono un archivio e non vengono effettuat i backup - si rischia la perdita dei documenti);

Ad ogni Utente e ufficio viene assegnato uno spazio di condisione file server:

- **Personali e di servizio:** costiuisce buona prassi effettuare con cadenza periodica la pulizia degli spazi di archivi presenti nelle cartelle di rete di propria competenza, con cancellazione di file inutili e obsoleti. Attenzione ad evitare un'archiviazione ridondante con duplicazione di dati.
- **Le aree di scambio file:** ricordiamo che le aree di scambio file non sono aree pensate e strutturate da funzionare come archivio, ma sono aree di lavoro condivise che permettono il lavoro in team su un progetto o che permettono lo scambio di file tra colleghi come funzione di intranet interna. Quando le pratiche sono concluse vanno archiviate o, se sono già archiviate, devono essere rimosse da queste aree per non creare doppioni. In particolare l'area di Scambio_Utenti sarà resettata automaticamente trimestralmente.

In caso di comprovato pericolo per la sicurezza dei sistemi, l'Ente potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni presenti negli spazi di condivisione degli Utenti, dandone successiva e tempestiva comunicazione agli interessati.

In caso di assenza programmata o cessazione della sua attività lavorativa presso l'Ente, al fine di garantire la continuità del servizio, l'Utente ha l'obbligo di rendere disponibile la relativa documentazione sugli spazi di condivisione file server del proprio servizio.

Inoltre, in caso di cessazione, verranno disattivate prontamente le credenziali dell'Utente da parte dell'Amministrazione di Sistema. I backup dello spazio file server personale sono conservati dall'Amministratore di Sistema presso l'Ente per n.6 mesi prima della sua definitiva cancellazione.

4.13 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.)

L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative. Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica antivirus, per permettere al sistema di completare la verifica di sicurezza che non può essere interrotta dall'Utente. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, per non danneggiare e rendere illeggibili i dati.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto la responsabilità dell'utilizzatore, che è tenuto a rivolgersi al Servizio CED per le opportune configurazioni di sicurezza e/o crittografia del dispositivo.

È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

L'Utente è tenuto a informare immediatamente i dirigenti responsabili della struttura organizzativa di appartenenza, il Servizio CED e il Responsabile della Protezione dei Dati, anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

Alcune raccomandazioni di buon senso:

- I supporti rimovibili (CD, DVD, pen drive, schede di memoria, hard disk rimovibili, etc.) devono essere custoditi con la massima diligenza e riservatezza e non devono essere lasciati incustoditi o facilmente accessibili.
- Nel momento in cui l'Utente non ha più bisogno del supporto, sia esso riscrivibile o non riscrivibile (ad esempio: CD-R, DVD-R, DVD+R, CD-RW, DVD-RW, DVD+RW, pen drive, schede di memoria, hard disk rimovibili, etc.), è tenuto a restituirlo al Servizio CED.

4.14 Strumenti di firma digitale

La firma digitale è utilizzata per la sottoscrizione di documenti informatici nell'ambito delle attività istituzionali dei soggetti abilitati e nel rispetto dei poteri di firma derivanti dalla legge o dai regolamenti interni dell'Ente.

Il titolare del certificato di firma digitale è tenuto a:

a) adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma, che utilizzerà personalmente e per ragioni istituzionali;
b) conservare con la massima diligenza e riservatezza i propri codici personali al fine di evitarne l'uso fraudolento da parte di terzi;
c) comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione all'incaricato del servizio di firma digitale ed informarlo dell'eventuale variazione del rapporto contrattuale con l'Ente e di tutti i dati richiesti per l'emissione del certificato;
d) informare anticipatamente gli incaricati del servizio di firma digitale di ogni circostanza che renda necessaria o, comunque, opportuna la revoca o la sospensione del certificato e del dispositivo di firma a lui assegnato; deve altresì informare tempestivamente il suddetto incaricato di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

4.15 Comportamenti non consentiti

Sono vietati a tutti gli Utenti i seguenti comportamenti:

a) l'utilizzo abusivo di credenziali altrui, la cessione a terzi delle credenziali di utilizzo di firma digitale (o strumento equivalente), l'accesso non autorizzato a risorse informatiche dell'Ente e/o lo scambio di comunicazioni mediante falsa identità;
b) l'installazione, sulla PdL in dotazione, di software non coperto da licenza o, comunque, non preventivamente autorizzato dal Servizio CED;
c) l'utilizzo, per comunicazioni personali, di chat, social network o altri strumenti di comunicazione aziendale messi a disposizione dall'Ente;
d) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;
e) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);
f) il mantenimento delle PdL accese al termine della giornata lavorativa;
g) la modifica delle configurazioni di base dei dispositivi assegnati dall'Ente senza l'autorizzazione preventiva del Servizio CED (non è possibile, ad esempio, configurare account privati nel client di posta);
h) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

4.16 Protezione contro furti e danneggiamenti

Tutte le PdL portatili e i dispositivi mobili devono essere custoditi in luogo sicuro, adottando le opportune precauzioni contro il furto delle strumentazioni informatiche e/o dei dati in esse contenuti.
L'Utente è tenuto a informare immediatamente il dirigente responsabile, il Servizio CED e, qualora vi sia la possibilità di una violazione di dati personali, altresì il RPD di qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

5. CONTROLLI E MONITORAGGI

In ottemperanza a quanto stabilito dall'art. 4 del d.lgs. 300/1970, non vengono nel modo più assoluto utilizzate apparecchiature/strumentazioni hardware e software al fine di consentire controlli a distanza, prolungati, costanti o indiscriminati dei lavoratori.

È quindi nel pieno rispetto dei principi di pertinenza e di non eccedenza ed evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, che l'Ente si riserva di effettuare controlli e monitoraggi sull'uso degli strumenti informatici messi a disposizione per lo svolgimento dell'attività lavorativa e sul presupposto di un utilizzo responsabile degli stessi da parte degli Utenti, adottando in ogni caso le soluzioni tecnologiche idonee a garantire i profili di sicurezza dei sistemi informativi e dei dati gestiti. Detti controlli sono svolti esclusivamente dalla Struttura competente per la gestione dei sistemi informativi.

A tal fine, l'Ente utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "file di log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici dell'Ente e delle informazioni ivi contenute, come indicato nel Paino della Sicurezza Informatica e analisi dei rischi dell'Ente. Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log relativi alla navigazione possono essere esaminati dall' Amministratore di Sistema per l'individuazione del problema tecnico e l'adozione delle necessarie misure conseguenziali. In ogni caso, tutti i controlli di funzionalità e monitoraggio avvengono nel rispetto di quanto previsto dal CAD, dalle norme in materia di tutela della libertà e dignità dei lavoratori, della normativa unionale e nazionale in materia di protezione dei dati personali.

L'Amministratore di sistema, nel caso in cui rilevi anomalie o configurazioni non corrette delle PdL, può provvedere a isolare immediatamente l'origine dell'anomalia o del malfunzionamento anche senza preavvisare l'Utente, per salvaguardare la sicurezza e l'integrità dei sistemi informativi dell'Ente. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento sulla PdL da parte dell'amministratore di sistema.

Gli eventuali controlli generali ed estesi atti a verificare condotte non conformi al presente Disciplinare avverranno preliminarmente su dati aggregati (c.d. "controllo anonimo") riferiti all'intera struttura lavorativa ovvero al Settore o alla Direzione qualora il Settore, per caratteristiche intrinseche alla struttura organizzativa, non offrisse garanzie di completa anonimità della verifica.

Nel caso vengano rilevate anomalie o irregolarità, potrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all'utilizzo corretto degli strumenti elettronici aziendali, nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Qualora le anomalie o le irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente all'area in cui è stata rilevata l'anomalia. In caso di ripetute anomalie o irregolarità si procederà a controlli su base individuale, su singoli nominativi, basi e postazioni.

Oltre a ciò, l'Ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Oltre a tali controlli di carattere generale, l'Ente si riserva comunque le facoltà di effettuare specifici controlli nel rispetto della normativa vigente.

6. MODALITA' DI GESTIONE BACKUP

La gestione dei backup viene effettuata dal Servizio Informatico afferente all'Area Servizi Generali, per ciò che riguarda i dati che risiedono presso l'Ente, e dai fornitori esterni per i servizi dati in concessione esterna o su cloud.

L'Ente provvede alla messa in sicurezza delle informazioni del Sistema Informatico attraverso la creazione di ridondanza delle informazioni stesse (backup dei dati), da utilizzare come recupero (ripristino) dei dati stessi in caso di eventi malevoli accidentali o intenzionali o semplice manutenzione del sistema.

L'Utente, per poter richiedere il ripristino dei propri dati mediante l'utilizzo delle copie di backup, deve farne richiesta ufficiale via mail al Servizio Informativo dell'Ente.

Incaricati alla copia, verifica e ripristino: Amministratore di Sistema

Periodicità:

- **BACKUP ARCHIVI:** mensile
- **BACKUP GENERALE SERVER AREE DI LAVORO IN USO:** giornaliero
- **BACKUP MAIL:** giornaliero

7. *RESPONSABILITÀ E SANZIONI*

La violazione del presente disciplinare e dei Codici di comportamento del personale può comportare l'applicazione delle sanzioni disciplinari previste dal decreto legislativo 30 marzo 2001, n. 165 e s.m.i., dai contratti collettivi applicabili al personale in servizio e dal singolo contratto di lavoro.

Resta ferma la responsabilità civile, penale e contabile di ogni Utente per fatti illeciti e/o danni derivanti da usi non consentiti della Rete o degli strumenti informatici messi a disposizione dall'Ente, anche alla luce delle prescrizioni contenute nel presente disciplinare.

8. *ALLEGATI*

Password e criteri di sicurezza
Pila Software
Utilizzo della posta elettronica da parte degli Utenti

Allegato - Password e criteri di sicurezza

Le password devono soddisfare i seguenti requisiti:

1 - Complessità:

I requisiti di complessità vengono verificati al momento della creazione o della modifica della password.

- Non possono contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente.
- Devono contenere caratteri appartenenti ad almeno tre delle quattro categorie seguenti:
    - Caratteri maiuscoli dell'alfabeto inglese (A-Z)
    - Caratteri minuscoli dell'alfabeto inglese (a-z)
    - Cifre decimali (0-9)
    - Caratteri non alfabetici, ad esempio !, $, #, % (facoltativo)

2- Lunghezza

- Lunghezza minima: 8 caratteri;
- lunghezza massima 14 caratteri

Alla password vengono applicati i seguenti criteri:

- Necessità di essere modificata al primo utilizzo
- Validità massima: 90 giorni
- Impossibilità di riuso delle ultime 24 password utilizzate

Allegato - Pila Software

Utilizzare software prettamente necessari all'attività lavorativa e fare attenzione a installare programmi di dubbia provenienza.

Annualmente l'Amminsitratore di sistema provvederà alla scansione dei software installati sulle Pdl dell'Ente, come da indicazione delle Misure minime di sicurezza imposte dal Piano dell'Informatica.

Elenco categorie software approvate:

- MS Windows
- GNU/Linux (Debian/Ubuntu/Redhat)
- Applicativi desktop per i servizi di file hosting (gdrive, dropbox, icloud, onedrive, ecc)
- Applicativi software per la navigazione Internet (Firefox, Chrome ecc..)
- Suite Office (Microsoft Office, LibreOffice, ecc)
- Software per la gestione di dispositivi e periferiche (es. software stampanti, scanner ecc)
- Software per l'amministrazione, per la didattica, la ricerca, gestione forestale, servizi tecnici (es. Siscom, QGIS ecc..)
- Software vari e tool per la gestione di file (es. iso, zip, pdf, jpeg, gif, avi, mpeg, ecc)
- Software per l'ottimizzazione del dispositivo (es. CCleaner)
- Software per la sicurezza del dispositivo (es. ESET Endpoint Security)
- Software per la modellazione 2D/3D (es. CAD)
- Software di accesso e amministrazione remota (vpn, desktop remoto, ssh, ecc)
- Software di virtualizzazione e emulazione (virtual box, vmware, bluestack, ecc)
- Software di streaming, videoconferenza e VoIP (es Zoom, Cisco, GoToMeeting ecc)
- Software per la firma digitale (es. GoSign ecc)
- Software per la grafica (es. Suite Adobe, Gimp, Paint ecc)
- DBMS e Web server (MySQL, Apache)
- Password manager
- Gestionali LLPP

Prima di installare un nuovo softawe consultare il Servizio CED.

Inoltre le *Linee guida acquisizione e riuso di software per le pubbliche amministrazioni* (https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa) indirizzano le stesse nel processo decisionale per l'acquisto di software, la condivisione e il riuso delle soluzioni open source.

Di seguito i link utili per la valutazione di utilizzo di software a riuso della PA:
http://www.riuso-pa.piemonte.it/cms/
https://developers.italia.it/

Allegato - Utilizzo della posta elettronica da parte degli Utenti

L'Utente è tenuto ad osservare le seguenti indicazioni:

1. ogni comunicazione dovrà riportare i seguenti elementi essenziali:
   a. oggetto;
   b. contenuto (testo ed eventuale allegato/i);
   c. firma.
2. i messaggi di posta elettronica, inviati verso l'esterno devono riportare in calce la "firma standard", secondo il seguente formato base:

   Nome Cognome - Carica
   ENTE DI GESTIONE DELLE AREE PROTETTE DEI PARCHI REALI
   Sede Legale: Viale Carlo Emanuele II, 256 - 10078 Venaria Reale (TO) - Sede operativa di Stupinigi: viale Torino 4, (fraz. Stupinigi) – 10042 Nichelino (TO
   Tel. servizio - Cell. Servizio se presente
   pec: parchireali@legalmail.it

   Il presente messaggio contiene informazioni di natura professionale attinenti all'attività lavorativa. Ai fini dello svolgimento dell'attività lavorativa le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Questo messaggio di posta e il suo contenuto sono riservati e confidenziali e destinati esclusivamente al soggetto indicato nell'indirizzo. Se per errore riceverete questo messaggio o non siete il soggetto destinatario o delegato dal destinatario alla lettura, Vi preghiamo di darcene immediatamente notizia e quindi di cancellare definitivamente il messaggio di posta elettronica.

Le stesse indicazioni valgono anche per le caselle di **posta elettronica certificata PEC.**