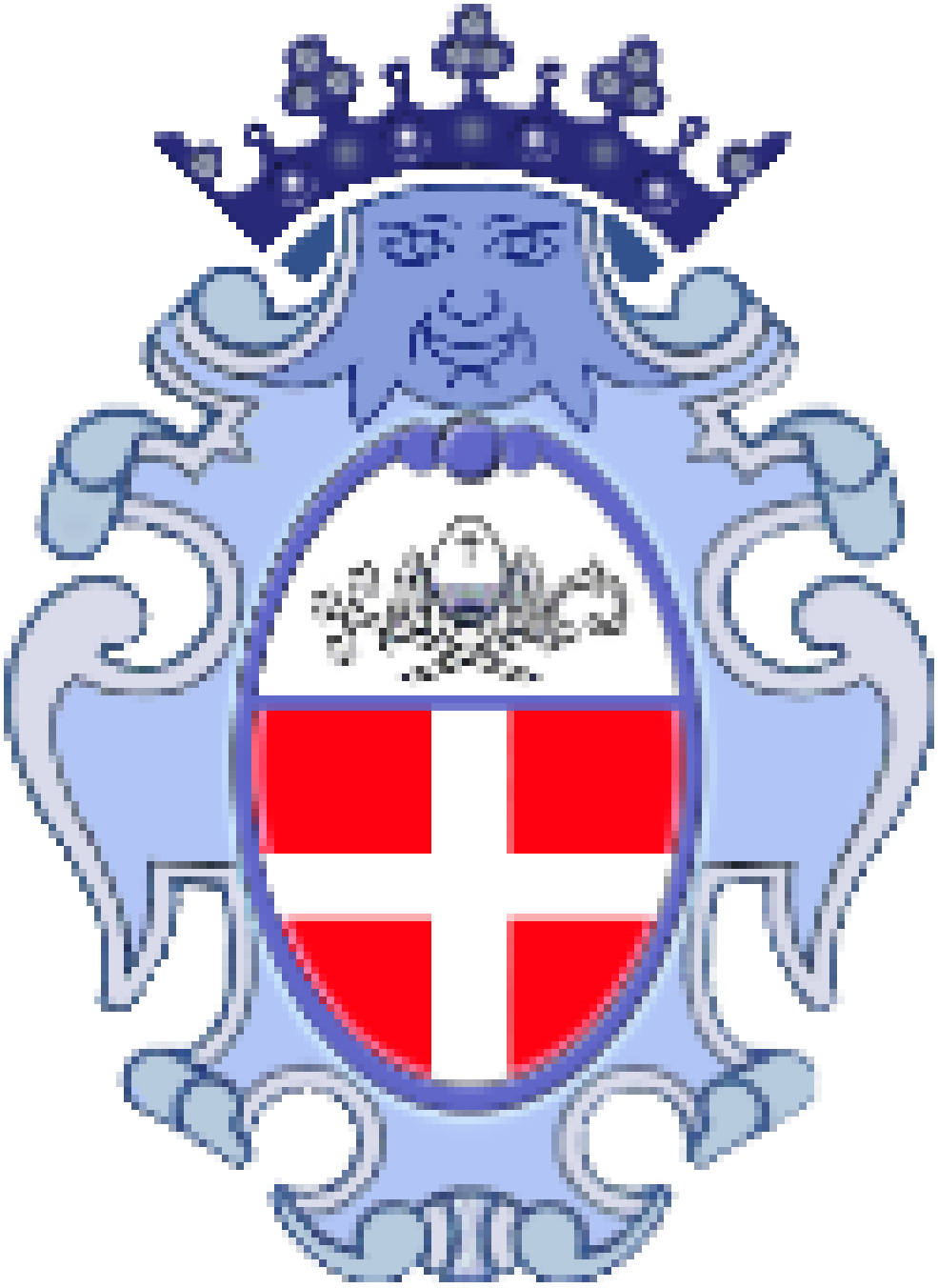
a



Disciplinare interno per l’utilizzo degli strumenti informatici

a

Sommario

1. Introduzione 4

1.1 Finalità del documento 4

1.2 Contesto normativo 5

2. Glossario e Definizioni 6

3. Principi generali 8

4. Regole per l'utilizzo dei sistemi informatici dell'ASP 9

4.1 Credenziali di autenticazione al dominio 9

4.2 Utilizzo di applicazioni aziendali 10

4.3 Postazione di lavoro 11

4.4 Postazione di lavoro portatile 13

4.5 Altri dispositivi 13

4.6 Software a corredo 13

4.7 Navigazione in internet 14

4.8 Posta elettronica 15

4.9 Servizi di chat, messaggistica, videoconferenza, telefonia 17

4.10 Servizi Cloud e Spazi di condivisione di rete aziendale 17

4.11 Dispositivi di memorizzazione rimovibili (Hard disk, Pen drive USB, etc.) 19

4.12 Strumenti di firma digitale 20

4.13 Comportamenti non consentiti 20

4.14 Protezione contro furti e danneggiamenti 21

4.15 Comportamento in caso di assenza programmata 21

5. Controlli e Monitoraggi 22

a

5.1 Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni 23

6. Responsabilità e sanzioni 24

a

1. INTRODUZIONE

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

Il presente disciplinare deve considerarsi integrato da tutte le procedure interne adottate in ASP, fra cui la procedura prevista in caso di violazione di dati personali.

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 operative;
- 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 da ASP 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.

a

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 ASP;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito GDPR)

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 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/programma 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 NoiPA, abbonamenti a servizi informativi, portale ANAC, SMAF, DsP-Flux 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;

- ***Postazione di lavoro (PdL)****:* personal computer (desktop o portatile) messo a disposizione da ASP 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 di lavoro in essere a qualsiasi titolo con l'Agenzia, siano autorizzati all'utilizzo degli strumenti informatici messi a disposizione da ASP.

a

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 di ASP 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 ASP, 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 da ASP.

a

4. REGOLE PER L'UTILIZZO DEI SISTEMI INFORMATICI

4.1 Credenziali di autenticazione al dominio

L'accesso alle applicazioni del sistema informativo di ASP 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 in Agenzia implementa le seguenti regole:

- composizione di password complesse, che abbiano una lunghezza minima stabilita e una sequenza di caratteri normali, speciali e/o numerici;
- modifica della password al primo utilizzo;
- validità minima e massima della password;
- impossibilità di riuso delle ultime password utilizzate;
- blocco dell'utenza dopo un determinato numero di tentativi falliti di inserimento della password;
- reinizializzazione (reset) della password e riattivazione delle utenze disabilitate, secondo le procedure in vigore.

4.2 Utilizzo di applicazioni aziendali

L'accesso alle applicazioni aziendali e il loro utilizzo devono avvenire secondo le regole dettate dal presente Disciplinare, con riferimento ai diversi ruoli di responsabilità specificamente individuati in ASP 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 di ASP, ferma restando la disabilitazione all'usodegli applicativi e delle funzionalità di ASP da parte dell'Ufficio Referenti informatici interni, è fatto obbligo di restituzione delle strumentazioni elettroniche (pc portatili, tablet, cellulari, kit di firma elettronica ecc.) già affidate per l'esplicazione delle funzioni connesse al rapporto di lavoro.

In caso di assegnazione temporanea del personale ASP presso altra pubblica amministrazione, la titolarità della casella di posta elettronica sul dominio di ASP potrà essere mantenuta nel rispetto delle disposizioni che regolano l'uso di tale risorsaai sensi del presente disciplinare. All'atto dell'assegnazione temporanea e durante il relativo periodo di servizio, l'Ufficio Referenti informatici interni provvede alla disabilitazione all'uso degli applicativi e funzionalità, fermo restando l'obbligo del dipendente di restituzione della strumentazione informatica già assegnata da ASP perlo svolgimento della prestazione lavorativa.

4.3 Postazione di lavoro

Le postazioni di lavoro (PdL) sono gestite dal Servizio Referenti informatici interni 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 software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.).

L'assegnatario della PdL è profilato come utente senza diritti amministrativi.

La PdL è provvista del software base approvato da ASP. In caso di particolari necessità, è disponibile una lista di software, la cui installazione può essere richiesta direttamente dall'Utente al Servizio Referenti informatici interni tramite l'Helpdesk. Ulteriori necessità lavorative potranno essere rappresentate al Servizio Referenti informatici interni, che valuterà l'ammissibilità delle richieste.

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

a) la PdL è assegnata all'Utente per lo svolgimento della propria attività lavorativa; è consentito l'uso promiscuo, sia lavorativo sia personale, delle PdL ma nei limiti consentiti dalle normative vigenti e con responsabilità dell'Utente.

b) la PdL non deve essere accessibile a soggetti non autorizzati;

c) l'Utente non deve apportare modifiche alle configurazioni della PdL che non siano state preventivamente richieste e autorizzate dal Servizio Referenti informatici interni;

d) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa sugli spazi di condivisione aziendali;

e) durante l'allontanamento dalla PdL, l'Utente deve bloccare la propria postazione per consentirne l'accesso unicamente mediante l'immissione della password;

f) al termine della giornata lavorativa, soprattutto per motivi di sicurezza, deve essere effettuato lo spegnimento delle PdL.

4.4 Postazione di lavoro portatile

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

Si evidenzia che le stazioni di lavoro portatili, utilizzate al di fuori di ASP, sono maggiormente esposte a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutti gli Utenti, pertanto, devono custodire con cura e diligenza la postazione di lavoro portatile assegnata.

Le postazioni di lavoro portatili devono essere verificate dal Servizio Referenti informatici interni per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. Laverifica avviene mediante appuntamento concordato con il Servizio stesso. In caso di significativo rischio di compromissione o/e sicurezza, tale Servizio può richiedereall'Utente lo spegnimento della PdL portatile fino a tale verifica ovvero bloccare il dispositivo da remoto.

4.5 Altri dispositivi

Con riferimento ad altri dispositivi assegnati ai dipendenti, quali smartphone e/o tablet, valgono le medesime regole comportamentali adottate per le PdL.

4.6 Software a corredo

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.

Non è permessa l'installazione di software aziendale con licenza ASP su dispositivi privati.

4.7 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 di ASP.

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;
- trasferire sul proprio computer (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 di ASP 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 di ASP.

Al fine di prevenire l'accesso a siti web e risorse internet potenzialmente nocivi, per la navigazione dalla rete aziendale l'Agenzia adotta soluzioni di sicurezza basate su filtri e decriptazione delle informazioni della navigazione Internet (ad esclusione di determinate categorie di siti individuati da ASP, ad esempio siti bancari, sanitari, ecc.) 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,

siti per adulti) 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'Agenzia 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.

4.8 Posta elettronica

Tutti gli Utenti sono dotati di una casella di posta elettronica sul dominio di ASP. Le caselle devono essere utilizzate per l'esercizio della propria attività lavorativa.
L'utilizzo della casella PEC istituzionale è gestita dalla Direzione generale e dal Servizio Archivio/Protocollo ed il servizio che ne necessità l'utilizzo è coordinato dal dirigente di riferimento. Laddove vi fosse la necessità di istituire caselle PEC nominali queste devono essere utilizzate esclusivamente per motivi di ufficio in conformità alle regole del presente disciplinare e alle disposizioni impartite dal dirigente responsabile.

Quando si utilizza lo strumento della posta elettronica, è opportuno osservare comportamenti consoni.

Il sistema di posta elettronica prevede:

- ☐ per le e-mail inviate a destinatari esterni al dominio di posta elettronica di ASP, 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 dei messaggi mediante strumenti automatici, 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;
- 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.

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

- inserire la propria firma utilizzando il format definito da ASP per l'invio di messaggi verso l'esterno, uniformando il carattere del corpo del testo e la firma automatica in calce all'email secondo lo stile contenuto nel manuale di Firma e-mail ASP disponibile nel sito Intranet aziendale;
- 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 di ASP 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 in ASP;

- 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'Agenzia;
- 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 di ASP, indirizzi di posta elettronica di altri colleghi, per motivi non legati all'attività lavorativa.

ASP ha definito specifiche modalità per assicurare la disponibilità di informazioni in caso di assenza improvvisa o prolungata di un Utente. Fermo restando che i contenuti delle e-mail sono ordinariamente consultabili esclusivamente da parte dell'Utente titolare della casella, vengono adottate le seguenti misure di tipo tecnologico:

- possibilità di attivazione da parte dell'Utente, in caso di sua assenza prolungata, della funzione di risposta automatica con invito al mittente a prendere contatto con l'Ufficio competente di ASP.

4.9 Servizi di chat, messaggistica, videoconferenza, telefonia

L'utilizzo della messaggistica istantanea (Whatsapp…) e la creazione di gruppi per lo scambio di informazioni contenenti dati sensibili degli utenti di ASP è radicalmente incompatibile con l'uso aziendale, perché seppur crea immediatezza nello scambio di informazioni, crea un rapporto contrattuale diretto da dipendente e gestore del servizio (bypassando l'azienda). Inoltre divulga indiscriminatamente i dati dei partecipanti alle chat e non consente al datore di lavoro di supervisionare il trattamento dei dati relativi alla clientela messo in atto dai dipendenti.

Per la creazione di stanze virtuali di chat o audio/videoconferenza, siti, gruppi e relativi canali di condivisione, è necessario chiedere la preventiva autorizzazione al Servizio Referenti informatici interni.

4.10 Servizi Cloud e Spazi di condivisione di rete aziendale

Gli ***spazi di condivisione*** file server devono essere utilizzati per la memorizzazione di file ad uso strettamente lavorativo. 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, ovvero sui server aziendali e non debbono essere salvati in locale, sulla pdL.

In caso di comprovato pericolo per la sicurezza dei sistemi, ASP 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.
Alcune cartelle o file possono essere salvate su spazi comuni quali “canon” ecc.. ma solo per il tempo necessario alla loro lavorazione. Al termine della procedura connessa e l’avvenuta registrazione al protocollo della documentazione, tali cartelle o file debbono essere eliminati dagli spazi suddetti.

4.11 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 Referenti informatici interni 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 Referenti informatici interni 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 Referenti informatici interni.

4.12 Strumenti di firma digitale

L'uso del kit di firma digitale, anche remota, è strettamente personale e non cedibile a terzi.

4.13 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 della smart card di firma digitale (o strumento equivalente) ad esempio carta SISS, l'accesso non autorizzato a risorse informatiche di ASP 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 Referenti informatici interni;

c) l'utilizzo, per comunicazioni personali, di chat, social network o altri strumenti di comunicazione aziendale messi a disposizione da ASP;

d) l'utilizzo, per comunicazioni di servizio, di chat, social network o altri strumenti di comunicazione non aziendali;

e) l'utilizzo, la distruzione, l'alterazione o la disabilitazione non autorizzata di file e di ogni altra risorsa informatica;

f) l'allontanamento dalle PdL senza la preventiva adozione di opportune precauzioni di sicurezza (ad es. il blocco della PdL);

g) il mantenimento delle PdL accese al termine della giornata lavorativa;

h) la modifica delle configurazioni di base dei dispositivi assegnati da ASP senza

l'autorizzazione preventiva del Servizio Referenti informatici interni (nonè possibile, ad esempio, configurare account privati nel client di posta);

i) l'utilizzo di strumenti volti a eludere i sistemi di protezione.

4.14 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 Infrastrutture interne ICT e, qualora vi sia la possibilità di una violazione di dati personali, altresì qualsiasi danno, furto o perdita di strumentazioni informatiche, software e/o dati in proprio possesso, fermi restando gli obblighi di denuncia alle autorità competenti.

4.15 Comportamento in caso di assenza programmata

In caso di assenza programmata, al fine di garantire la continuità del servizio, l'Utente si impegnerà a: 1) rendere disponibile, ove necessario, la relativa documentazione su una share condivisa dell'ufficio; 2) attivare eventualmente la funzione di risposta automatica, utilizzando un messaggio contenente il periodo di assenza e l'eventuale contatto alternativo.

a

5. CONTROLLI E MONITORAGGI

ASP imposta la propria azione di monitoraggio e controllo sui sistemi informatici di ASP messi a disposizione per lo svolgimento dell'attività lavorativa nel rispetto dellanormativa vigente 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.

A tal fine, ASP utilizza sistemi automatizzati per la gestione centralizzata dei cosiddetti "filedi log", che consentono di tracciare eventuali anomalie o minacce informatiche che potrebbero colpire i sistemi, compromettendo la funzionalità e la sicurezza degli apparati informatici di ASP e delle informazioni ivi contenute.

I file di log relativi alla navigazione in internet sono registrati e conservati per le suddette finalità di funzionalità e sicurezza, in conformità alla normativa vigente e alle disposizioni adottate al riguardo da ASP, vedi allegato **File di Log**. Nel caso di eventi anomali e/o pregiudizievoli per la sicurezza informatica, i file di log file relativi alla navigazione possono essere esaminati dagli amministratori 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 europea 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 di ASP. In tal caso, verrà data successiva informativa all'Utente sui motivi dell'avvenuto intervento sulla PdL da parte dell'amministratore di sistema.

Le predette attività sono svolte nel rispetto dei principi di gradualità, pertinenza e non eccedenza stabiliti dal Garante per la protezione dei dati personali nonché dei diritti e delle libertà fondamentali dei lavoratori, sempre mediante funzionalità consentite dalla normativa vigente.

a

5.1. Ruolo degli amministratori delle risorse tecnologiche condivise e delle applicazioni

Gli Amministratori delle risorse tecnologiche condivise e delle applicazioni svolgono le attività necessarie per garantire la salvaguardia del sistema informativo e delle applicazioni conformemente alle politiche e alle istruzioni impartite da ASP e nel rispetto della normativa vigente con particolare riferimento alla protezione dei dati personali.
Qualora si renda necessario procedere a operazioni finalizzate al ripristino della funzionalità del Sistema informativo comportanti l'accesso a cartelle, file o archivi di altri Utenti, gli Amministratori sono tenuti a preavvisare gli interessati, limitando il proprio intervento a quanto strettamente necessario.

a

6. 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 da ASP, anche alla luce delle prescrizioni contenute nel presente disciplinare.