Provincia di Perugia

**SERVIZIO PIANIFICAZIONE TERRITORIALE, AMBIENTE,
SISTEMI INFORMATIVI E COMUNICAZIONE**

DISCIPLINARE UTILIZZO PC, ATTREZZATURE E SERVIZI INFORMATICI

INDICE

1 - PREMESSE E PRINCIPI GENERALI

L'esigenza della Provincia di Perugia di adottare un disciplinare per l'utilizzo dei personal computer fissi e portatili, dei dispositivi mobili, della rete telematica, della posta elettronica, internet e dei servizi informatici in genere, nasce dall'ormai consolidato uso di tali strumenti nell'organizzazione e nell'espletamento dell'attività lavorativa.
In applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., l'utilizzo di tali indispensabili risorse deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo tra l'Ente e i propri dipendenti.
Un utilizzo non avveduto di tali strumenti espone la Provincia di Perugia, gli utenti, dipendenti e collaboratori della stessa, a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge, quali, fra tutte, la legge sul diritto d'autore e quella sulla protezione dei dati, creando evidenti problemi alla sicurezza e all'immagine dell'Ente.
Il disciplinare è adottato per assicurare la funzionalità e il corretto impiego dei personal computer fissi e portatili, dei dispositivi elettronici in generale, della posta elettronica, di internet, da parte dei lavoratori sia in sede che a distanza: a tale fine, definisce le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa tenendo conto della disciplina in tema di diritti, relazioni sindacali e normativa sulla protezione dei dati (GDPR – NIS2).
Nel luogo di lavoro è assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati, garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Costituzione, art. 2087 c.c., art. 2, comma 5, Codice dell'amministrazione digitale, d.lgs. 7 marzo 2005, n. 82 e s.m.i.).
A tal fine l'Ente individua in maniera trasparente, con il presente disciplinare, anche le modalità di controllo sul corretto utilizzo delle strumentazioni utilizzate, garantendo che gli stessi si svolgano con procedure atte a salvaguardare il diritto alla riservatezza e alla dignità dei lavoratori, come sanciti dallo Statuto dei lavoratori e dal d.lgs. 30.6.2003, n.196, Codice in materia di protezione dei dati personali e s.m.i.
Le disposizioni e le prescrizioni qui indicate vanno affiancate ed integrano, quelle già previste nel Regolamento Generale sulla Protezione dei dati (GDPR - (UE) 2016/679), Regolamento sui criteri e le modalità organizzative (approvato con Deliberazione del Consiglio Provinciale n. 33 del 20.09.2022) e nella Direttiva Europea n. 2555 del 2022 c.d. "Direttiva NIS 2".

2 - CAMPO DI APPLICAZIONE

2.1 Il disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori della Provincia di Perugia, a prescindere dal rapporto contrattuale con la stessa intrattenuto (es. collaboratori esterni, collaboratori a progetto, stagisti, consulenti, borsisti ecc.).

2.2 Le disposizioni del presente disciplinare, che non siano espressamente destinate ai soli dipendenti o collaboratori, sono estese a tutti coloro che utilizzano attrezzature informatiche della Provincia di Perugia, nonché a qualsiasi utente autorizzato ad accedere alla sua rete telematica.

2.3 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi chiunque utilizza le attrezzature informatiche o la rete telematica della Provincia.

3 - UTILIZZO DEL PERSONAL COMPUTER

3.1 Il personal computer (p.c.) affidato all'utente è uno strumento di lavoro e deve essere considerato esclusivamente un "bene strumentale" disponibile per le attività autorizzate in funzione del ruolo, delle mansioni e dei compiti svolti. Ogni utilizzo non inerente le attività autorizzate dal presente disciplinare può determinare una violazione dei propri doveri d'ufficio con la relativa apertura di un procedimento disciplinare.

3.2 L'accesso al personal computer, ai programmi applicativi e alle varie funzionalità messe a disposizione degli utenti per lo svolgimento della loro attività avviene previa autenticazione, che consiste nella verifica dell'identità degli stessi attraverso l'uso di un codice identificativo (username) e di una parola chiave (password). La password deve essere custodita dall'utente con la massima diligenza e non divulgata. Per le regole ulteriori in merito alle credenziali di accesso si rimanda al capitolo (4) del presente disciplinare.

3.3 Solo il personale che opera presso il Sistema Informativo, amministratori di sistema o tecnici dallo stesso delegati, sono autorizzati a compiere interventi tecnici hardware e software sia per l'installazione che per la manutenzione su tutti gli apparati informatici di proprietà dell'Ente. Gli stessi tecnici sono altresì autorizzati, ai fini di verifiche funzionali e sicurezza del sistema, ad intervenire sui p.c. senza necessità di ulteriore autorizzazione.

3.4 I tecnici del Sistema Informativo possono collegarsi per effettuare interventi in teleassistenza e/o in desktop remoto alle singole postazioni (p.c.), previo consenso dell'utente, al fine di garantire l'assistenza tecnica e la normale attività operativa. In caso di oggettiva necessità e urgenza, a seguito della rilevazione di problemi nel sistema informatico e telematico, e in caso di prolungata assenza dell'utente, è consentito l'accesso al p.c. da parte dei tecnici dello stesso servizio.

3.5 Salvo preventiva espressa autorizzazione del Responsabile del Sistema Informativo, non è consentito all'utente modificare le caratteristiche di configurazione hardware e software impostate sul proprio p.c. né procedere ad installare programmi e/o dispositivi.

3.6 L'installazione e l'uso di programmi diversi da quelli installati dal Sistema Informativo, se legali, non dannosi ed utili all'incarico, viene consentita previa autorizzazione scritta del Responsabile del Sistema Informativo. Non viene consentito agli utenti installare autonomamente programmi provenienti dall'esterno, allo scopo di evitare il grave pericolo di introdurre Virus informatici o di alterare la funzionalità delle applicazioni software esistenti.

3.7 L'installazione di programmi da parte dell'utente, ove sia consentito dalle relative impostazioni (diritti di amministratore), deve avvenire nel pieno rispetto delle condizioni che ne disciplinano l'utilizzo e, in generale, della normativa vigente, con particolare riferimento alle disposizioni in materia di protezione di diritti di proprietà intellettuale. Abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro. In ogni caso, l'utente sarà responsabile e la Provincia è manlevata da qualsiasi danno o richiesta di risarcimento già da ora.

3.8 Non è consentito il collegamento di qualsiasi dispositivo USB nei p.c., salvo casi specifici, su richiesta esplicita del Dirigente, adeguatamente motivata da ragioni di servizio.

3.9 Tutti i software caricati sul sistema operativo e in particolare i software necessari per la protezione dello stesso o della rete internet, quali antivirus, firewall, ecc., non devono essere disinstallati o in alcun modo manomessi dall'utente.

3.10 In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), l'utente non deve lasciare il sistema operativo aperto con la propria password. Lasciare un p.c. incustodito connesso alla rete può essere infatti causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Al fine di evitare che persone estranee effettuino accessi non consentiti, è stata predisposta di default l'attivazione del salvaschermo con password dopo 10 min di inattività. L'utente può attivare questo blocco anche autonomamente, utilizzando i tasti CTRL+ALT+CANC).

3.11 L' utente è tenuto al pieno rispetto della normativa vigente per l'uso e l'accesso delle risorse tecnologiche (server, workstation, personal computer fissi e portatili, apparati di rete attivi e passivi). In particolar modo è tenuto:

- a non tentare deliberatamente di accedere abusivamente al sistema informatico o telematico di terzi protetto da misure di sicurezza, raggiungibile telematicamente tramite le risorse tecnologiche dell'Ente (art. 615 ter c.p.); a non far uso delle risorse tecnologiche per archiviare, detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- a non utilizzare le risorse tecnologiche per far uso, archiviare, detenere, duplicare o diffondere in qualunque forma materiali tutelati da diritti d'autore o diritti connessi o sui quali terzi vantano diritti morali e/o patrimoniali (d.lgs. 68/2003, legge 22 Aprile 1941, n.633 e successive modificazioni);
- a non far uso delle risorse tecnologiche al fine di eludere le eventuali misure tecnologiche di protezione poste a presidio di materiali tutelati da diritti d'autore o diritti connessi o sui quali terzi vantano diritti morali e patrimoniali (d.lgs. n. 68/2003, legge 22 Aprile 1941, n.633 e successive modificazioni);
- a non fare copie di software, applicazioni, librerie di supporto, documenti e quant'altro sia riferibile o faccia parte delle risorse tecnologiche e sia tutelato da diritti d'autore o diritti connessi o su cui terzi vantino diritti morali e patrimoniali (d.lgs. 68/2003, legge 22 Aprile 1941, n.633 e successive modificazioni), ove questa possibilità non sia prevista esplicitamente dalle licenze di uso (GNU General Public License, GNU Library General Public License, Artistic License, BSD e BSD-style, etc.);
- a non utilizzare le risorse tecnologiche per archiviare, detenere o diffondere in qualunque forma materiale pornografico, in particolare quello minorile (artt. 600 ter c.p. e 600 quater c.p.);
- a non utilizzare le risorse tecnologiche al fine di alterare o tentare di alterare il funzionamento dei servizi, delle stesse risorse tecnologiche o di qualsivoglia altro sistema informatico o telematico di terzi raggiungibile telematicamente tramite le risorse tecnologiche (art. 640 ter c.p.);
- a non utilizzare le risorse tecnologiche per archiviare, consegnare o diffondere programmi diretti a danneggiare o interrompere i servizi, le stesse risorse tecnologiche o qualsivoglia altro sistema informatico o telematico di terzi raggiungibile telematicamente tramite le risorse tecnologiche dell'Ente;
- a non utilizzare le risorse tecnologiche per intercettare, impedire o interrompere fraudolentemente le comunicazioni tra le stesse o tra qualsivoglia altro sistema informatico o telematico di terzi raggiungibile telematicamente tramite le risorse tecnologiche (art. 617 quater c.p.);

- a non utilizzare le risorse tecnologiche per attentare all'integrità di sistemi informatici o telematici di pubblica utilità (art. 420 c.p.);
- a non distruggere, deteriorare o rendere in tutto o in parte inservibile una risorsa tecnologica o qualsivoglia altro sistema informatico o telematico di terzi raggiungibile telematicamente tramite le risorse tecnologiche dell'Ente (art. 635 bis c.p.).

L'elenco deve considerarsi non esaustivo e restano tutti gli obblighi e divieti previsti dalla specifica normativa in vigore.

4 - GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

4.1 Le credenziali di autenticazione per l'accesso alla rete, ai p.c. ed alle applicazioni, vengono assegnate e trasmesse dal personale del Sistema Informativo. Per i dipendenti o collaboratori ciò avviene al momento in cui il relativo atto di nomina, indipendentemente dalla tipologia di rapporto instaurato, è perfezionato e inserito nello "Stato Giuridico" dell'Ente. Allo stesso modo, quando viene cessato dallo "Stato Giuridico" per dimissioni, pensionamento, licenziamento ecc., l'utente di rete assegnato viene disabilitato. Periodicamente, e comunque almeno annualmente, saranno verificate le credenziali di autenticazione e saranno disattivate quelle non utilizzate da più di 6 mesi.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (username), assegnato dal Sistema Informativo, associato ad una parola chiave (password) creata dall'utente, che dovrà essere riservata e custodita con la massima diligenza.

4.3 Le credenziali assegnate per l'accesso in VPN sono del tipo a doppio fattore (MFA), in quanto, oltre a username e password viene richiesta conferma dell'accesso tramite cellulare. L'ente si riserva di estendere questa tipologia di gestione degli accessi anche all'autenticazione a p.c. e servizi interni alla rete dell'ente.

4.4 Di ogni e qualsivoglia attività riconducibile all'uso di username (nome utente) è responsabile unicamente l'utente;

4.5 Il personale della Provincia, senza distinzione di ruolo e livello, nonché in generale gli utenti delle risorse informatiche e telematiche della Provincia, non sono in alcun modo autorizzati a richiedere la password relativa ad altro account utente.

4.6 Nel proprio interesse, l'utente è tenuto prontamente a comunicare al personale del Sistema Informativo, l'eventuale perdita di riservatezza e confidenzialità delle credenziali del proprio account utente, in modo da attivare le procedure necessarie per il cambio.

4.7 La password trasmessa dal Sistema Informativo dovrà essere cambiata dall'utente al primo accesso e, successivamente, quando richiesto dalla procedura automatizzata.

4.8 Per una completa ed esaustiva guida alla creazione e gestione delle credenziali si rimanda all'allegato "B" del presente disciplinare.

5 – UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE LOCALI E DI RETE

5.1 I documenti e i file non devono essere mantenuti all'interno del disco fisso del pc, ma devono essere obbligatoriamente trasferiti nelle piattaforme appositamente predisposte secondo le modalità specifiche di ognuna. Questo permette di prevenire le violazioni dei dati personali che possano comportare, accidentalmente o in modo illecito, la sottrazione e/o la perdita per danneggiamento del disco fisso, attacco ransomware, esfiltrazione;

5.2 L'ente, al fine di attuare un'organizzazione più funzionale e per prevenire possibili violazioni, mette a disposizione dell'utente alcune piattaforme dove archiviare i file, sia per le attività amministrative che per quelle tecniche. Le piattaforme sono regolate dalla normativa e dai Dirigenti del Servizio che le gestiscono.

5.3 Per l'ottimizzazione degli spazi di archiviazione e per non appesantire le procedure di sicurezza, i dati archiviati nelle piattaforme devono contenere informazioni strettamente professionali, di particolare importanza o riservatezza. Va invece evitato che queste siano utilizzate come destinazione provvisoria dei file.

5.4 L'accesso alle piattaforme sarà legato all'attività professionale di ogni dipendente ed autorizzato dietro formale richiesta effettuata dal dirigente al responsabile della piattaforma. Sarà cura del dirigente comunicare per iscritto eventuali cambi di mansione o trasferimenti e comunque ogni circostanza che comporti variazione in merito agli utenti autorizzati;

5.5 Tutti i dati/file salvati su disco locale, al di fuori dello spazio di rete di cui al punto 5.1 e della cartella "Personale" già presente nel desktop, sono disponibili per tutti coloro che accedono direttamente al p.c. anche se utilizzano credenziali (username/password) diverse. Comunque si evidenzia che al verificarsi di un guasto tecnico o attacco informatico, potrebbero essere persi e/o sottratti;

5.6 Secondo il principio della "Limitazione della Conservazione", applicato al trattamento dei dati, è buona regola che l'utente provveda alla cancellazione dei file al conseguimento delle finalità per le quali sono trattati;

5.7 Il personale del Sistema Informativo può, in qualunque momento, procedere alla rimozione di ogni file o applicazione ritenuti pericolosi per la sicurezza o difformi dalle autorizzazioni emanate, dal presente disciplinare e dalle norme vigenti, sia sui p.c. che sulle unità di rete. Dopo la rimozione sarà comunicato all'interessato l'evento e le ragioni che lo hanno generato.

6 – UTILIZZO DEI COLLEGAMENTI DI RETE DELLA PROVINCIA

6.1 Il collegamento alla rete viene garantito a tutti gli utenti che ne hanno necessità per lo svolgimento della loro attività lavorativa. Questo permette l'accesso alla rete Locale e Geografica e alle applicazioni e piattaforme;

6.2 Gli utenti non possono collegare alla rete telematica dell'Ente personal computer, notebook,

palmari o simili, provenienti dall'esterno;

6.3 Ogni connessione di rete ha una specifica configurazione che ne identifica l'ubicazione e la funzione. È obbligatorio interpellare il Sistema Informativo prima di ogni spostamento di p.c. per valutare l'impatto, la fattibilità e predisporre le configurazioni adeguate;

6.4 Gli armadi di rete contengono apparati fondamentali che distribuiscono le informazioni sulla rete informatica fisica delle sedi della Provincia. È proibito a chiunque, escluso il personale del Sistema Informativo, l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto;

6.5 In caso di malfunzionamenti è necessario, per il personale tecnico, poter accedere agli apparati tempestivamente. È quindi vietato depositare materiale nelle vicinanze degli armadi di rete e nel raggio d'azione della porta di accesso all'armadio, con particolare riferimento a sostanze infiammabili;

6.6 È responsabilità di ogni utente prestare attenzione a non alterare le connessioni a muro e i cavi che le collegano ai p.c. con sedie e arredi.

7 – UTILIZZO P.C. PORTATILI

7.1 L'utente è direttamente responsabile del p.c. fisso, portatile e di qualsiasi altro dispositivo assegnatogli dall'Ente e deve custodirlo con diligenza e utilizzarlo con la massima cura, adottando, in caso di allontanamento, tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni. Il compito di controllo della conformità di utilizzo di cui al presente articolo da parte dell'utente è demandato al Dirigente del Servizio cui l'utente è assegnato;

7.2 Ai p.c. portatili si applicano le regole di utilizzo previste dal presente disciplinare per i personal computer collegati alla rete dell'Ente, con particolare attenzione all'installazione e utilizzo di software e APP nel rispetto della normativa vigente in materia di protezione dei diritti di proprietà intellettuale. L'assegnatario del dispositivo sarà chiamato a rispondere personalmente per eventuali violazioni;

7.3 Per quanto riguarda la navigazione e l'utilizzo di servizi internet dal pc portatile, in considerazione del fatto che il dispositivo naviga senza il controllo degli apparati di sicurezza dell'ente, l'assegnatario è direttamente responsabile della navigazione e utilizzo di internet;

7.4 I pc portatili, al momento della restituzione, saranno resettati e riportati alle impostazioni di fabbrica, cancellando tutti i dati contenuti. Pertanto sarà l'assegnatario che, prima della restituzione, provvederà all'eventuale copia dei dati.

8 – PROTEZIONE ANTIVIRUS MALWARE E SOFTWARE MALEVOLI

8.1 Tutti i p.c. fissi e portatili dell'Ente sono protetti da software antivirus e anti-malware aggiornato quotidianamente tramite la rete telematica dell'Ente. Ogni utente deve comunque tenere

comportamenti tali da ridurre il rischio di attacchi da virus ed altri software “malevoli”;

8.2 Non è consentito collegare o ricollegare alla rete p.c. fissi e portatili che siano stati scollegati dalla stessa per almeno 6 mesi. L’apparecchiatura deve essere visionata dal personale del Sistema Informativo, che ne autorizza il collegamento;

8.3 Tutti gli utenti della rete telematica dell’Ente, per garantire la sicurezza del sistema, sono dotati di privilegi limitati. Per poter accedere al p.c. con i privilegi di amministratore, l’utente, sotto la propria responsabilità e con congruo anticipo, non inferiore a due giorni, deve richiedere l’assegnazione di tali diritti indicando il motivo. I diritti saranno assegnati temporaneamente per il solo periodo necessario a consentire l’attività dichiarata. Nel caso in cui i diritti di amministratore siano utilizzati per attività diversa da quella riportata sulla richiesta, l’utente sarà chiamato a rispondere in caso di danni all’Ente o a terzi.

9 – MODALITA’ DI EROGAZIONE DELL’ASSISTENZA

9.1 Il Sistema Informativo è l’unico referente per qualsiasi problematica riguardante aspetti legati all’informatica, (software di base, RDBMS e software applicativi specifici acquisiti dal sistema informativo), alla rete telematica dell’Ente, sia locale che geografica ed alla telefonia fissa e mobile;

9.2 Il Sistema Informativo eroga prevalentemente i seguenti servizi, sempre vigilando adeguatamente sul rispetto delle direttive e delle norme vigenti:

- gestione della manutenzione operativa (aggiornamento delle vulnerabilità e delle revisioni) sistema operativo e dell’hardware, per quanto disponibile e/o sottoposto a contratti di manutenzione, anche per mezzo di personale esterno;
- configurazione e installazione di nuovi dispositivi e applicazioni software, nonché supporto tecnico-logistico per la corretta installazione e configurazione da parte di personale esterno, quando previsto;
- gestione operativa degli “account utente” della rete, utenti abilitati all’accesso delle risorse e delle banche dati;
- gestione di tutti gli apparati telematici a cui la rete della Provincia è collegata, anche per mezzo di personale esterno.

9.3 Il Sistema Informativo fornisce inoltre assistenza tecnica per installazione, configurazione e manutenzione di tutti i p.c. dell’Ente. A tale scopo gli utenti sono tenuti a seguire le istruzioni appresso indicate.

- In caso di sostituzione del p.c. funzionante, l’utente è tenuto preventivamente a organizzare i dati relativi alla propria attività lavorativa e ad effettuare le copie degli stessi. È inoltre onere dell’utente salvare ed eliminare i dati riconducibili alla propria sfera personale.
- Sarà a cura dell’utente indicare in forma iscritta i file e le cartelle da trasferire nel nuovo p.c.
- Saranno altresì trasferite tutte le cartelle di servizio di competenza del Sistema Informativo.
- Tutto il restante contenuto residente nel p.c. d’origine, non espressamente comunicato dall’utente al tecnico come riconducibile all’attività lavorativa, non verrà trasferito e non sarà più disponibile.
- E’ onere dell’utente presiedere alle operazioni di salvataggio dei propri documenti, la perdita di

dati dovuta ad errore umano (utente/tecnico) nel corso dell'assistenza non può dar luogo ad azioni di rivalsa di nessun genere.

Nel caso in cui gli addetti del Sistema Informativo debbano intervenire sul p.c. per motivi tecnici l'utente deve garantire la disponibilità entro 2 gg lavorativi dalla richiesta, altrimenti il p.c. sarà disattivato;

9.4 Tutte le richieste di assistenza tecnica devono essere inviate tramite il form all'uopo predisposto all'interno della intranet. Non sono consentite altre forme di richiesta (salvo i casi in cui il sistema è indisponibile). Le richieste inviate tramite il form consentono una gestione efficiente e efficace da parte dei tecnici;

9.5 Per effettuare le attività di assistenza/supporto, i tecnici del Sistema Informativo possono avvalersi di un sistema di teleassistenza. Questa viene attivata, nei casi di routine o comunque senza carattere d'urgenza, dopo la richiesta dell'utente, contattando l'utente stesso comunicando la connessione al p.c. L'utente ha la possibilità e l'onere di visionare tutte le attività svolte da remoto e in ogni momento può interrompere la teleassistenza;

9.6 I tecnici del Sistema Informativo o il personale esterno incaricato di svolgere attività di assistenza tecnica sono tenuti al rispetto dell'art. 622 del c.p;

9.7 Gli accessi effettuati dal personale del Sistema Informativo o dal personale esterno incaricato, per svolgere l'attività di assistenza tecnica non possono configurarsi come una violazione della privacy, compresi gli accessi alla posta elettronica.

10 – USO DELLA POSTA ELETTRONICA

10.1 La casella di posta, assegnata dall'Amministrazione Provinciale all'utente, è uno strumento di comunicazione elettronica da utilizzare per l'attività lavorativa. Gli assegnatari delle caselle di posta elettronica sono direttamente responsabili del corretto utilizzo delle stesse;

10.2 Nel caso sia necessario condividere fra più utenti i messaggi ricevuti, è disponibile una casella di con caratteristiche di "lista di distribuzione". L'indirizzo di posta come lista di distribuzione (ufficioxxx@provincia.perugia.it; progettoxxx@provincia.perugia.it) permette di far ricevere in maniera del tutto indipendente e riservata lo stesso messaggio a più caselle di posta individuale (nome.cognome@provincia.perugia.it) assegnate ai dipendenti di ruolo;

10.3 Allo scopo di rendere edotti gli interlocutori circa la natura non privata della casella di posta elettronica, i messaggi devono contenere un avvertimento ai destinatari del seguente tenore letterale:

"Il presente messaggio di posta elettronica con gli eventuali allegati contiene informazioni di natura professionale attinenti l'attività lavorativa. Esso è rivolto unicamente alla persona fisica o giuridica alla quale è indirizzato e può contenere informazioni riservate e confidenziali. Ai fini dello svolgimento dell'attività lavorativa, le eventuali risposte, potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Si rammenta inoltre che il messaggio è protetto dalla legge sia ai sensi dell'art. 616 c.p. che delle vigenti norme in materia di protezione dei dati personali (D. Lgs. 196/2003, D. Lgs. 101/2018, Regolamento UE 679/2016): pertanto, se il lettore non è il destinatario diretto o la persona incaricata alla consegna del messaggio al destinatario diretto, si avvisa che qualsiasi diffusione, distribuzione o copia della presente comunicazione e dei documenti

eventualmente allegati è vietata. In caso di ricezione di questa mail per errore, si prega di notificare immediatamente il disguido al mittente e cancellare il messaggio ed ogni allegato"

10.4 Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e proporzionalità, il sistema, in caso di assenze programmate, consente l'invio automatico di messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto. In caso di assenza non programmata o di impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per improrogabili necessità legate all'attività lavorativa sia necessario accedere ai messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare un altro dipendente a sua scelta, regolarmente in servizio ("delegato"), all'apertura della posta. Il dipendente "delegato" ha il compito di verificare il contenuto dei messaggi e inoltrare a chi di competenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Della nomina e del passaggio delle credenziali al "delegato" è redatto apposito verbale da parte di quest'ultimo e del responsabile del Servizio, che alla prima occasione utile sarà sottoscritto anche dall'utente assente. In ogni caso il "delegato" è responsabile di ogni attività riconducibile all'uso dell'username dell'utente legittimo assegnatario fino a che questi non rientri in servizio e non chieda l'immediata sostituzione della password;

10.5 È diretta responsabilità dell'utente il preventivo controllo di eventuali file allegati ai messaggi di posta elettronica prima del loro scarico e utilizzo, in relazione a rischi e ai danni che ne possono derivare;

10.6 È vietato inviare, trasmettere o diffondere pubblicità, materiale promozionale, "junk mail", "spam", "catene di S.Antonio", "piramidi" o qualsiasi altra forma di sollecitazione non autorizzata o non richiesta;

10.7 Non è consentito effettuare acquisti on line e ogni genere di comunicazione finanziaria. È ammesso assolvere, senza allontanarsi dal luogo di lavoro, adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero detenere rapporti con istituti bancari e assicurativi o in generale compiere incombenze amministrative e burocratiche on line, esclusivamente per il tempo necessario per l'espletamento delle transazioni, secondo quanto riportato nella direttiva n. 2/09 del Dipartimento della Funzione pubblica;

10.8 Non è consentito simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta non proprie, per l'invio di messaggi; creare intestazioni o in altro modo manipolare segni distintivi o indicazioni al fine di contraffare l'origine di un contenuto trasmesso o diffuso tramite il servizio di posta elettronica;

10.9 Non è consentito l'utilizzo di crittosistemi o di qualsiasi altro programma di sicurezza o crittografia non previsto dalla legge o non autorizzato dal Sistema Informativo;

10.10 L'utente non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:

- contenuti che siano illeciti, dannosi, minatori, abusivi, molesti, diffamatori e/o calunniosi, volgari, osceni, lesivi della privacy altrui, razzisti, classisti o comunque reprensibili;
- materiale pornografico o simile o in violazione della Legge n. 269/1998 "Norme contro lo

sfruttamento sessuale dei minori";

- contenuti che non abbia il diritto di trasmettere o diffondere in forza di una previsione di legge, di contratto ovvero a causa di un rapporto fiduciario (per esempio informazioni riservate, informazioni confidenziali apprese in forza del rapporto di lavoro o protette da un patto di riservatezza);
- contenuti che comportino la violazione di brevetti, marchi, segreti, diritti di autore o altri diritti di proprietà industriale e/o intellettuale dell'Ente o di terzi soggetti;
- comunicazioni commerciali private;
- materiali che violino le norme sulla privacy;
- pubblicità non istituzionali, manifeste o occulte
- altri contenuti illegali;

10.11 L'utente, nell'uso del servizio di posta elettronica e del proprio indirizzo e-mail è tenuto altresì a rispettare quanto disposto dal capitolo 3 del presente disciplinare.

11 – USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

11.1 Il p.c. assegnato al singolo utente ed abilitato alla navigazione Internet, costituisce uno strumento necessario allo svolgimento dell'attività lavorativa;

11.2 L'utente è sempre personalmente responsabile della propria attività di navigazione. Non è permesso l'accesso e la navigazione in internet tramite la rete telematica dell'Ente se non per fini esclusivamente lavorativi e professionali, o comunque consentiti, ivi compresi quelli di cui al capoverso (10.7). Non è permesso modificare la configurazione dei p.c. fissi o portatili, installata per la navigazione internet;

11.3 E' fatto divieto all'utente lo scarico (download) di files, software gratuiti (freeware e shareware) se non pertinenti alla propria attività lavorativa. In tutti gli altri casi deve esserne fatta esplicita richiesta di autorizzazione al Responsabile del Sistema Informativo;

11.4 E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività professionale di ciascun utente;

11.5 E' vietata la partecipazione e l'iscrizione a social network, forum e l'utilizzo di "chat line" a "bacheche elettroniche", la registrazione in guest books, anche utilizzando pseudonimi (nicknames), quando non direttamente riconducibili all'attività lavorativa di ciascun utente;

11.6 Non è consentito scaricare o scambiare materiale coperto da diritto d'autore;

11.7 L'utente è tenuto ad utilizzare, per accedere alla rete, soltanto computer di proprietà dell'Ente, salvo espressa autorizzazione ad utilizzare un computer privato. Tutti gli strumenti informatici saranno utilizzati esclusivamente per scopi lavorativi; ogni diverso utilizzo è vietato;

11.8 Al fine di evitare upload, download, navigazione in siti il cui contenuto non è pertinente con le attività o finalità dell'Ente, si è provveduto ad attivare un sistema di filtraggio che blocca l'accesso a detti siti. I Dirigenti di Servizio possono richiedere per iscritto al Responsabile del

Sistema Informativo l'accesso e la navigazione in siti bloccati ma comunque riconducibili alle attività e finalità dell'Ente;

11.9 E' vietato a chiunque manomettere o eludere i sistemi di sicurezza e/o filtraggio alla navigazione attivati dal Sistema Informativo;

11.10 **I log di navigazione saranno rilevati e conservati per un massimo di 6 mesi per finalità di sicurezza** nel rispetto di quanto disposto dal DPR n. 81 del 13/06/2023;

11.11 A seguito di ripetute e significative anomalie, l'Amministrazione Provinciale può svolgere verifiche sui dati inerenti l'accesso alla rete dei propri dipendenti o collaboratori. I servizi e gli utenti interessati al controllo dovranno essere preventivamente messi a conoscenza delle motivazioni specifiche alla base dei controlli;

11.12 Il dipendente o collaboratore è comunque tenuto a utilizzare internet nel rispetto delle leggi vigenti e prestando particolare cautela al fine di non importare virus, spam o altri programmi informatici dannosi;

11.13 L'utente non può utilizzare proprie postazioni di lavoro per collegarsi alla rete Internet o installare su P.C. fissi o portatili di proprietà dell'Amministrazione Provinciale dispositivi o apparati che consentano il collegamento alla rete senza l'autorizzazione al Responsabile del Sistema Informativo.

12 – ASSEGNAZIONE E UTILIZZO DEL SERVIZIO VPN (VIRTUAL PRIVATE NETWORK)

12.1 L'attivazione della VPN avviene solo su specifica richiesta del Dirigente del Servizio a cui il dipendente è assegnato. La VPN viene assegnata per particolari istituti di lavoro a distanza quali smart working, lavoro da remoto e simili;

12.2 Il Dirigente, che ne ha richiesto l'attivazione, dovrà anche provvedere a chiederne la disattivazione al venir meno dei presupposti che ne hanno originato l'attivazione;

12.3 L'attivazione della VPN è subordinata all'assegnazione al dipendente della strumentazione informatica fissa o mobile di proprietà dell'ente e del necessario token per la verifica a doppio fattore. Il dipendente dovrà firmare per accettazione il verbale con le specifiche prescrizioni, come da allegato C, parte integrante del presente disciplinare. L'allegato C sarà modificato ogniqualvolta cambino i riferimenti normativi che regolano i vari istituti di lavoro a distanza e/o le misure di sicurezza informatica da applicare;

12.4 Per l'applicazione delle misure di sicurezza il dipendente accetta di utilizzare l'APP su dispositivo mobile (smartphone) di servizio e, in caso ne fosse sprovvisto, su quello personale in applicazione dell'articolo 12, comma 3-Bis del decreto legislativo 7 marzo 2005 n. 82;

12.5 La strumentazione informatica sarà configurata dai tecnici del sistema informativo e/o da ditta incaricata, l'utente non è autorizzato a nessun tipo di modifica;

12.6 Nel caso di istituti di lavoro a distanza in cui il collegamento internet è a carico del dipendente, lo stesso dovrà provvedere al collegamento della strumentazione assegnata alla linea e garantire l'adeguatezza tecnologica e funzionalità per consentire il buon esito del collegamento VPN.

13 – OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY.

13.1 E' obbligatorio attenersi alle disposizioni di volta in volta emanate dall'Amministrazione Provinciale e dalle autorità competenti in materia di protezione dei dati e delle misure di sicurezza, volte a garantire l'integrità dei sistemi e delle piattaforme.

14 – CONTROLLI

14.1 L'Amministrazione Provinciale, nella sua qualità di datore di lavoro, si riserva la facoltà di effettuare controlli in conformità alla vigente normativa e nel rispetto delle "Linee guida del Garante per posta elettronica e Internet" e della direttiva della Presidenza del Consiglio - Dipartimento della Funzione Pubblica n. 2/2009 avente per oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro";

14.2 L'Amministrazione Provinciale rispetta il principio di proporzionalità dei controlli, che si concretizza nella pertinenza e non eccedenza delle attività di controllo. Le limitazioni della libertà e dei diritti individuali devono essere proporzionate allo scopo perseguito. E' esclusa la possibilità di controlli prolungati, costanti ed indiscriminati.
I predetti controlli si svolgeranno in forma graduata, come segue:

- in via preliminare, sull'evidenza di anomalie, l'Amministrazione Provinciale provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura lavorativa ovvero ai servizi e dunque ad un controllo anonimo che si concluderà con un avviso generalizzato inerente al rilevato utilizzo anomalo dei dispositivi elettronici, della posta elettronica e di internet;
- in assenza di successive anomalie non si effettueranno controlli su base individuale;
- nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro informando gli interessati del tipo di controllo a cui sono sottoposti ed esplicitando le specifiche attività non consentite;

14.3 Se nel corso di tali controlli viene rilevato un non corretto utilizzo degli strumenti informatici messi a disposizione dall'Ente da parte dei singoli utenti, si procederà all'invio di un avviso all'utente ed al Dirigente del Servizio Interessato ed eventualmente al DPO. Sarà cura del Dirigente del Servizio interessato segnalare l'evento all'Ufficio per i procedimenti disciplinari per l'adozione degli atti di rispettiva competenza. Per il personale dirigente il comportamento verrà segnalato al Direttore Generale, se nominato, altrimenti al Segretario Generale che procederà secondo quanto previsto dal CCNL vigente;

14.4 Oltre a tali controlli di carattere generale, l'Amministrazione Provinciale si riserva comunque la facoltà prevista dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che hanno causato danno all'amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.

15 - SANZIONI

15.1 E' fatto obbligo a tutti gli utenti di osservare le disposizioni del presente disciplinare. La violazione delle regole e dei divieti di cui al presente disciplinare costituisce, per i dipendenti, violazione del Codice di comportamento e comporta l'irrogazione delle sanzioni disciplinari proporzionali al danno ed alla violazione, previste dalla normativa e dal vigente CCNL, fatte salve tutte le azioni civili e penali;

15.2 Il mancato rispetto delle regole e dei divieti del presente disciplinare costituisce, per i collaboratori esterni, violazione degli obblighi contrattuali e li espone alle azioni penali e civili consentite.

16 – AGGIORNAMENTO E REVISIONE

16.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente disciplinare. Le proposte verranno esaminate dal punto di vista della fattibilità tecnica dal Responsabile del Sistema Informativo e successivamente, se ritenute attuabili, seguiranno l'iter di aggiornamento previsto dalle procedure dell'Ente e saranno rese note a tutti i dipendenti;

16.2 Il presente disciplinare è soggetto a revisione periodica in concomitanza con significative esigenze tecniche o operative o per adeguamenti normativi.

17 – ENTRATA IN VIGORE E TRASPARENZA

17.1 Il disciplinare entrerà in vigore il giorno successivo alla data di esecutività della deliberazione di approvazione;

17.2 Con l'entrata in vigore del presente disciplinare, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti;

17.3 L'Amministrazione provinciale assicura la massima trasparenza alle disposizioni contenute nel presente disciplinare, con particolare riferimento alle procedure di controllo in esso previste. A tal fine copia del disciplinare, verrà pubblicata nel sito istituzionale e sulla rete Intranet e verrà trasmesso per e mail a tutti i dipendenti. L'adempimento delle suddette modalità costituisce "informativa" nei confronti di tutti i dipendenti e collaboratori ai sensi e per gli effetti dell'art.13 del d.lgs. 196/2003;

17.4 Il presente disciplinare è articolato in specifici allegati che possono essere oggetto di modifica e/o aggiornamento, approvati con determina del Responsabile del Sistema Informativo.

17.5 Per quanto non regolamentato dal presente disciplinare si rimanda alla normativa vigente in materia di protezione dei dati e alle misure per aumentare il livello di sicurezza delle reti e dei sistemi (GDPR – NIS2).

ALLEGATO A
Glossario e definizioni

<u>Glossario generale</u> desunto da fonti pubbliche e "Open Source" (es. Wikipedia), al fine di rendere più completa e chiara l'interpretazione dei termini utilizzati nel presente disciplinare.

Account Utente sono le credenziali composte dalla coppia "Username" e "Password" tramite le quali un Utente è identificato univocamente dai sistemi e per mezzo delle quali ha l'autorizzazione ad accedere ai Servizi erogati dalle Risorse Tecnologiche.

Autenticazione, nel campo della sicurezza informatica, si definisce (trad. Greco: αυθεντικός, da 'authentes'='autore') il processo tramite il quale un computer, un software o un utente destinatario, verifica che il computer, il software o l'utente dal quale esso ha ricevuto una certa comunicazione sia realmente il mittente che sostiene di essere.

Backup, nell'informatica indica un'importante operazione tesa a duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sulle unità di memorizzazione di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita (per esempio una volta al giorno o alla settimana). L'attività di backup è un aspetto fondamentale della gestione di un computer: in caso di guasti o manomissioni, il backup consente, infatti, di recuperare i dati dell'utente o degli utenti che utilizzano la postazione; in caso di server o di database, questo recupero può essere essenziale per il lavoro di molte persone.

Banca dati (vedi Database)

Bios (del p.c.), codice informatico, parzialmente personalizzabile, che presiede al funzionamento e configurazione di base dei dispositivi e delle periferiche di un elaboratore, accedibile attraverso opportuni comandi all'accensione dell'elaboratore stesso. Consente modifiche sostanziali di configurazione dell'elaboratore stesso e l'impostazione a vario livello di password di blocco d' accesso e/o funzionamento che possono compromettere il normale utilizzo dell'elaboratore, pertanto deve essere gestito, salvo eccezioni specifiche, esclusivamente da personale tecnico autorizzato e non da utenti / utilizzatori.

Chat Il termine (in inglese, letteralmente, "chiacchierata"), è usato per riferirsi ad un'ampia gamma di servizi sia telefonici che via Internet; ovvero, complessivamente, quelli che i paesi di lingua inglese distinguono di solito con l'espressione "online chat", "chat in linea". Questi servizi, anche piuttosto diversi fra loro, hanno tutti in comune due elementi fondamentali: il fatto che il dialogo avvenga in tempo reale, e il fatto che il servizio possa mettere facilmente in contatto perfetti sconosciuti, generalmente in forma essenzialmente anonima.

Credenziali di accesso - autenticazione Il termine si riferisce alla combinazione di due o più informazioni riservate, comunemente "username" o "utente" e "password", conosciute da un utente / utilizzatore di un personal computer e/o di una rete informatica, che consentono l'accesso univoco (riconducibile esclusivamente a chi le possiede / conosce) e profilato (abilita esclusivamente l'accesso a dati e applicazioni abilitate dal Titolare) alle risorse del computer e/o della rete stessa.

Crittografia tecnologia informatica che consente proteggere con una “chiave” di codifica normalmente inviolabile, dati, documenti e/o messaggi tra due o più utenti / utilizzatori e di renderli nel contempo indecifrabili a quanti non sono in possesso di opportune “chiavi” per la decifrazione.

Database Il termine, tradotto in italiano con *banca dati*, *base di dati* (soprattutto in testi accademici) o anche basedati, indica un insieme di dati riguardanti uno stesso argomento, o più argomenti correlati tra loro, strutturata in modo tale da consentire che i dati possano venire utilizzati per diverse applicazioni e, normalmente, possano evolvere nel tempo.

E-commerce, o commercio elettronico consiste nella compravendita, nel marketing e nella fornitura di prodotti o servizi attraverso computer collegati in rete. Nell'industria delle telecomunicazioni si può intendere anche come l'insieme delle applicazioni dedicate alle transazioni commerciali.

Forum è un particolare strumento di comunicazione telematico in cui l'utente può scrivere dei messaggi (post) che saranno pubblicati in uno spazio comune insieme ai messaggi degli altri utenti. Ad ogni messaggio potranno seguire diverse risposte (reply), che seguiranno l'argomento del messaggio originario (topic), costituendo un thread, abbreviato in 3D.

Freeware, il termine indica un software che è distribuito in modo gratuito. Il freeware è distribuito indifferentemente con o senza codice sorgente, a totale discrezione dell'autore e senza alcun obbligo al riguardo. È sottoposto esplicitamente ad una licenza che ne permette la redistribuzione gratuita. Il software freeware è concesso in uso senza alcun corrispettivo, ed è liberamente duplicabile e distribuibile, con pochissime eccezioni.
Di norma l'autore che decide di rilasciare il suo lavoro come freeware, esercitando appieno il suo diritto di scegliere le forme e le modalità di distribuzione che ritiene più idonee, inserisce esplicitamente delle clausole che impediscono qualsiasi tipo di pagamento per la distribuzione del suo software, fatto salvo un eventuale "piccolo" rimborso per supporti e spese di duplicazione, esattamente come avviene per lo *shareware*.

Nickname o semplicemente nick, nella cultura di Internet, è uno pseudonimo o "nome di battaglia", usato dagli utenti di Internet per identificarsi in un determinato contesto o in una determinata comunità virtuale. Spesso sono soprannomi, ma possono essere sigle, combinazioni di lettere e numeri.

Risorse Tecnologiche tutti i server, le workstation, i personal computer, le periferiche (come ad esempio le stampanti, scanner, i sistemi di archiviazione, etc.) gestite sotto la responsabilità dell’ente, unitamente ad ogni dispositivo di rete sia attivo che passivo a cui tali sistemi posso essere interconnessi, compresi i sistemi per l'accesso ad Internet. A quanto sopra indicato si aggiungano software, applicazioni, librerie di supporto, documenti o servizi informatici connessi con i sistemi o le reti sopra indicate, così come la posta elettronica ed ogni altro servizio Internet.

Servizi è l’insieme di funzionalità che il Sistema Informativo mette a disposizione degli utenti.

Username o *nome utente* in informatica definisce il nome con il quale l'utente è riconosciuto da un computer, da un programma o da un server. In altre parole, esso è un identificativo che, insieme alla password, rappresenta le credenziali o account per entrare nelle risorse o in un sistema. L'uso di un

nome utente permette spesso anche di mantenere l'anonimato non rivelando il proprio nome reale: il nome utente prende in questo caso la funzione di pseudonimo.

Utenti sono tutti coloro che sono autorizzati all'uso dei Servizi (dipendenti, collaboratori, personale esterno,etc.).

Password (trad. "parola chiave", in italiano "parola d'ordine", o anche "parola d'accesso") è una sequenza di caratteri e numeri che viene usata per accedere in modo esclusivo ad una risorsa (sportello Bancomat, computer, connessione Internet, ecc). Ovviamente non è necessario che abbia senso compiuto e può essere costituita in alcuni casi anche da una frase.
Spesso si usa in coppia con un'altra parola, la User Id o Username (in italiano "Nome Utente") con il fine di far identificare in modo univoco dal sistema al quale chiediamo accesso, tra i tanti utenti che sono registrati su quel sistema.
La coppia di *Nome Utente* e *Parola d'accesso* rappresentano le "*Credenziali di Accesso*" ad un sistema e rappresentano una forma di *Autenticazione*.
La password dove rimanere riservata a coloro i quali non sono autorizzati ad accedere alla risorsa in questione.

Posta Elettronica Certificata (P.E.C.), è un servizio di posta elettronica che permette di ottenere la garanzia del ricevimento del messaggio da parte del destinatario. In italia oggi l'invio di una e- mail certificata (nelle forme stabilite dalla normativa vigente) è equiparato a tutti gli effetti di legge alla spedizione di una raccomandata cartacea con avviso di ricevimento (art. 48 del decreto legislativo 7 marzo 2005, n. 82). Ai fini della legge, il messaggio si considera consegnato al destinatario quando è accessibile nella sua casella di posta. La disciplina di dettaglio della posta elettronica certificata si trova nel DPR 11 febbraio 2005, n. 68.
Il meccanismo consiste nel fatto che il gestore di posta elettronica certificata, nel momento in cui prende a carico l'e-mail del mittente invia a lui una ricevuta di accettazione, che certifica l'avvenuto invio. Nel momento invece in cui il gestore deposita il messaggio nella casella del destinatario, invia al mittente una ricevuta di consegna che certifica l'avvenuta ricezione. Sia la ricevuta di accettazione che la ricevuta di consegna sono in formato elettronico, e ad esse è apposta la firma digitale del gestore.
Se il gestore di posta elettronica certificata del mittente è diverso dal gestore del destinatario, si ha un passaggio ulteriore: il gestore del destinatario, nel momento in cui riceve la mail dal gestore del mittente, emette una ricevuta di presa a carico, in formato elettronico, a cui appone la propria firma digitale. Se il gestore di posta elettronica non è in grado di depositare la mail nella casella del destinatario, invia una ricevuta di mancata consegna. I gestori di posta certificata hanno l'obbligo di non accettare le e-mail contenenti virus.

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. Nel nostro Ente i dirigenti sono "responsabili" della gestione e tutela dei dati personali trattati all'interno delle strutture cui sono direttamente preposti.

Shareware è una tipologia di licenza software molto popolare sin dai primi anni 90. Sono distribuiti sotto tale licenza in genere piccoli programmi facilmente scaricabili via Internet.
Il software sotto tale licenza può essere liberamente ridistribuito e utilizzato per un periodo di tempo di prova variabile (generalmente 30 giorni), dopodichè è necessario registrare il software presso la casa produttrice pagandone l'importo.

Spam, (detto anche fare spamming) è 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.

Titolare 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. Secondo questa definizione, titolare del trattamento dei dati personali di cui la Provincia dispone è la Provincia medesima nel suo complesso.

ALLEGATO B
Linee guida per la creazione e gestione delle credenziali di accesso

Introduzione
Le credenziali di accesso personali sono, prima di tutto, uno strumento che tutela l'utente dagli utilizzi illeciti dei propri privilegi di accesso alle risorse hardware, software e dati. La sua corretta scelta, seguita da una gestione mirata a preservare la riservatezza, è il modo migliore per garantire innanzitutto a se stessi, e quindi all'Ente, la tutela della parte di patrimonio informativo che ognuno è chiamato alla responsabilità di gestire.

Costruzione della password
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (USERNAME) associato a una parola chiave riservata, cioè conosciuta solamente dal medesimo (PASSWORD).
Ad ogni dipendente sono collegati individualmente un nome utente e una password.

Caratteristiche Nome Utente
Il nome utente (username) è assegnato dal "Servizio Sistema Informativo E-Government" ed è composto abbinando l'intero cognome più l'iniziale del nome del dipendente.
Esempio:
Nome dipendente: Bianchi Alfredo
Utente: BianchiA
Nel dominio di rete non è possibile avere "nomi utente" uguali. In caso di omonimia utente, (cognomi uguali e iniziali del nome uguali), a uno dei due nomi utente sarà aggiunta la secondo lettera del nome.
Esempio.
Nomi dipendenti: Bianchi Alfredo Bianchi Arturo
Utente: BianchiA BianchiAr
Il nome utente non è modificabile dal dipendente in quanto viene creato e attivato dal Sistema Informativo solo in presenza di un atto (nomina o similare) che ne attesti la qualità di dipendente o altro, pertanto autorizzato ad accedere ai servizi di rete della Provincia di Perugia.

Caratteristiche Password
La password è composta da almeno 10 caratteri. Deve
contenere:
almeno 1 carattere delle lettere maiuscole dell'alfabeto latino (dalla A alla Z) almeno 1 carattere delle lettere minuscole dell'alfabeto latino (dalla a alla z) almeno 1 carattere dei numeri in base 10 (da 0 a 9)
Opzionale caratteri non alfanumerici. Esempio: punto esclamativo (!), dollaro ($), simbolo di cancelletto (#) o percentuale (%).

Non deve contenere:
il nome utente o parte di esso. Esempio: Utente: BianchiA la password non può contenere il nome Bianchi o parte di esso.
riferimenti riconducibili all'incaricato o ai propri familiari. Esempio: data di nascita dell'incaricato o dei figli, nome proprio dei figli o della moglie/marito, ecc.

La procedura automatizzata implementata dal Sistema Informativo obbliga ogni 3 mesi al cambio della password e non permette l'utilizzo delle ultime 2 password inserite.

Conservazione delle credenziali di accesso

La password non deve essere rivelata a nessuno e deve essere custodita dal legittimo proprietario in maniera tale da evitare a chiunque di accedere alla sua conoscenza. In particolare è importante non scrivere la password su fogli, biglietti od oggetti che vengono lasciati in prossimità del p.c. (sul video, sopra o sotto la tastiera, ecc.). Se risulta indispensabile trascriverla per poterla ricordare è opportuno nasconderla tra le pagine dell'agenda o della rubrica telefonica senza comunque indicare che si tratta della propria password.

Sostituzione

E' importante tenere presente che la password consente l'accesso a dati personali o sensibili (presenze, busta paga) e pertanto è necessario provvedere alla sostituzione quando è stata rivelata o si sospetta che abbia perso il carattere di riservatezza.

ALLEGATO C
Prescrizioni e Responsabilità utilizzo attrezzatura informatica e accesso VPN

Introduzione

La VPN (Virtual Private Network) permette di collegarsi alla rete aziendale da remoto dalla propria abitazione o altro luogo e di svolgere le proprie mansioni lavorative anche se fisicamente non si è in ufficio. Infatti con il collegamento VPN è possibile utilizzare il pc dell'ufficio e tutte le piattaforme quali protocollo, contabilità, atti monocratici, presenze ecc. come se il dipendente fosse all'interno della sede di lavoro. La VPN viene attivata ai dipendenti a cui è stato riconosciuto lo status di lavoro agile e viene disattivata con il decadere di questo status. Per l'applicazione delle misure di sicurezza al dipendente viene assegnato un pc portatile di proprietà dell'ente all'uopo configurato e un token per la verifica delle credenziali a doppio fattore (MFA). Per permettere l'applicazione di questa misura di sicurezza, il dipendente si impegna in applicazione dell'articolo 12, comma 3-bis del decreto legislativo 7 marzo 2005 n. 82 ad utilizzare il cellulare personale se sprovvisto di quello di servizio. Inoltre il dipendente si impegna e sottoscrive le seguenti prescrizioni.

a) Il pc portatile deve servire esclusivamente per adempiere alle mansioni lavorative dell'assegnatario, dal momento della consegna non è ammesso l'utilizzo di strumentazioni diverse per il collegamento in VPN.
b) L'assegnatario si obbliga a conservare e a custodire il bene in oggetto con cura e massima diligenza, ed a non destinarlo ad altri usi che non siano quelli sopra previsti, a non cedere neppure temporaneamente l'uso del bene sopra individuato a terzi, né a titolo gratuito, né a titolo oneroso;
c) L'assegnatario è consapevole che la Provincia di Perugia non controlla in alcun modo l'attrezzatura, pertanto ogni file o cartella scaricata, ogni software/applicativo installati ricadono esclusivamente sotto la responsabilità dell'assegnatario.
d) Tutto il traffico sviluppato di qualsiasi natura (SMS, voce, internet, ecc…) verso qualsiasi direttrice/destinazione è integralmente sotto la responsabilità dell'assegnatario.
e) Il portatile è il mezzo per attivare e collegarsi al pc dell'ufficio pertanto non dovranno essere salvati o archiviati documenti nel disco fisso locale in quanto non si garantisce la sicurezza, l'integrità e in caso di riparazione/sostituzione non saranno copiati.
f) I tecnici della Provincia, visto che il portatile è solo un mezzo per collegarsi al pc dell'ufficio, garantiscono il loro supporto secondo le modalità di cui ai punti g) h) i) e solo se il portatile non funziona o non si collega alle VPN.
g) Per garantire la privacy non è prevista la teleassistenza, l'utente in caso di malfunzionamento del portatile dovrà recarsi presso gli uffici dei tecnici.
h) In caso di problemi con il collegamento in VPN il portatile dovrà essere recapitato ai tecnici che insieme al consegnatario provvederanno alle verifiche del caso.
i) Se i problemi di collegamento sono dovuti alla linea di proprietà del dipendente, lo stesso dovrà provvedere per garantirne l'affidabilità e la potenza necessaria.
j) L'assegnatario è l'unico responsabile di fronte all'autorità sia nel caso di smarrimento o furto.
k) L'assegnatario dichiara che il materiale ricevuto è integro, perfettamente funzionante e regolarmente utilizzabile.

Su richiesta scritta del Dirigente, adeguatamente motivata da ragioni di servizio, la VPN può essere attivata anche a dipendenti che per gravi motivi non possono recarsi in ufficio, ovviamente con le stesse misure di sicurezza e prescrizioni applicate per il lavoro agile.