PROVINCIA DI BRESCIA

Determinazione Dirigenziale n° 1656/2018

SETTORE DELLA INNOVAZIONE, DEL TURISMO E DEI SERVIZI AI COMUNI
Proposta n° 661/2018

OGGETTO: APPROVAZIONE DELLE LINEE GUIDA SULL'UTILIZZO DEGLI STRUMENTI E DEL SISTEMA INFORMATICO DELLA PROVINCIA DI BRESCIA.

IL DIRETTORE
(Ing. Raffaele Gareri)

Richiamati:

- la deliberazione del Consiglio Provinciale n. 7 del 24/04/2018, di approvazione del Bilancio di Previsione 2018-2020, del Documento Unico di Programmazione e del Piano degli indicatori del Bilancio 2018/2020 e successive variazioni;
- il decreto del Presidente della Provincia n. 113 del 22/05/2018 di approvazione del Piano Esecutivo di Gestione e delle Performance 2018/2020 e successiva variazione approvata con Decreto del Presidente n. 174 del 05/07/2018;
- il decreto del Presidente della Provincia n. 330 del 21/12/2017 di conferimento al sottoscritto, dell'incarico di direzione dell'Area delle Risorse e dello Sviluppo dell'Area Vasta, del Settore della Innovazione, del Turismo e dei Servizi ai Comuni e del Settore delle Risorse Umane e Controllo di Gestione e prorogato con successivo decreto n. 364 del 02/11/2018 fino al 01/02/2019;

Verificati:

- la coerenza del presente provvedimento con il Progetto PEG n. 011 "Gestione e sviluppo dell'infrastruttura e degli applicativi digitali dell'ente" - Obiettivo n. 317 "Manutenzione e assistenza ordinaria rete, telefonia, postazioni utente e applicativi, compresi quelli specifici di singoli settori. Adeguamento tecnologico, rinnovo dotazioni informatiche e telefoniche";
- il rispetto delle misure in materia di Trasparenza e di Prevenzione della Corruzione di cui al vigente Piano Triennale di Prevenzione della Corruzione, approvato con decreto del Presidente della Provincia n. 20 del 26 gennaio 2018;

Premesso che nell'obiettivo operativo delle Misure di Regolamentazione del Piano Triennale di Prevenzione della Corruzione, sopra indicato, relativamente al Settore della Innovazione, del Turismo e dei Servizi ai Comuni, costituisce indicatore di attuazione la predisposizione di Linee guida per l'utilizzo del sistema informativo provinciale, per il controllo e la tutela dello stesso, a fronte sia della sua complessità, sia della delicatezza dei dati e delle informazioni trattate;
Visto che il documento è stato redatto;
Considerato opportuno che venga approvato con idoneo provvedimento, come previsto dalla fase conclusiva dell'obiettivo gestionale in oggetto;
Visto l'art. 107 "Funzioni e responsabilità della dirigenza" del decreto legislativo 18 agosto 2000, n. 267 "Testo Unico degli Enti Locali";

Preso atto che il presente provvedimento è munito dei pareri previsti dall'articolo 147 bis del D. Lgs. n. 267/2000;

DETERMINA

di approvare le "Linee guida sull'utilizzo degli strumenti e del sistema informatico della Provincia di Brescia", in allegato, che costituiscono parte integrante e sostanziale del presente atto.

Brescia, lì 27-11-2018

Il IL DIRIGENTE
RAFFAELE GARERI

PROVINCIA
DI BRESCIA

Linee guida sull'utilizzo degli strumenti e del sistema informatico della Provincia di Brescia

(internet, posta elettronica, PC, telefoni e altri strumenti elettronici)

Indice generale

Art. 1. PREMESSE

La Provincia di Brescia, nell'ottica del raggiungimento di elevati livelli di efficienza, ha fatto un sempre maggiore ricorso alle tecnologie dell'informazione e della comunicazione, spinta anche dai complessivi processi di innovazione e dematerializzazione del procedimento amministrativo che hanno coinvolto tutta la Pubblica Amministrazione.

In tale contesto, anche le modalità di organizzazione della performance lavorativa hanno subito un profondo cambiamento, al punto che la maggioranza del personale, nello svolgimento delle quotidiane mansioni lavorative, fa uso di strumenti e servizi telematici, consulta o archivia documenti informatici, si connette a Internet e utilizza la posta elettronica.

In queste attività si possono individuare principalmente due momenti, nei quali può verificarsi un trattamento di dati personali. Il primo momento si concretizza in ragione dei contenuti dei documenti utilizzati, che possono riguardare individui identificati o identificabili. Il secondo momento è legato ai comportamenti degli utenti, le cui attività lasciano traccia all'interno dei sistemi preposti al funzionamento e alla protezione dell'infrastruttura di rete o all'interno dei dispositivi utilizzati. Queste tracce potrebbero contenere informazioni relative agli utenti o a terze persone, anche ricadenti nella sfera dei dati personali.

Sul tema dell'utilizzo appropriato degli strumenti informatici, in modo particolare della navigazione su internet e della posta elettronica, l'Autorità Garante della protezione dati personali ha emanato a più riprese alcuni provvedimenti, che si vanno ad integrare con il complesso della normativa in materia.

In considerazione del rapido evolversi delle norme in questione e della progressiva diffusione delle nuove tecnologie, vista la considerevole esposizione dell'Ente e degli utenti (dipendenti, collaboratori, fornitori, amministratori, ecc.) a molteplici rischi e a maggiori responsabilità, sia sul piano disciplinare, sia sul piano civile/penale, sia sul piano contabile, la Provincia di Brescia adotta le presenti “Linee guida”, con il quale si prefigge di fornire le necessarie informazioni a tutti i soggetti coinvolti, affinché possano, da un lato, conoscere ed esercitare i propri diritti e dall'altro apprendere le norme di comportamento da osservare nell'utilizzo degli strumenti informatici in uso onde evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei sistemi informatici e dei dati in essi conservati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento Europeo 2016/679 contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato inoltre che la Provincia di Brescia, nell’ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte attrezzature di vario genere (PC, computer portatili, telefoni cellulari, smartphone, tablet, stampanti di rete, etc.), sono state inserite nelle presenti “Linee guida” alcune clausole relative alle modalità e i doveri da osservare nell’utilizzo di tale strumentazione, sia sotto un profilo meramente tecnico-informatico sia sotto il profilo organizzativo.

Nelle presenti “Linee guida” si propone pertanto di prevenire comportamenti scorretti e/o illeciti, sintetizzando modalità e finalità di utilizzo del sistema informativo aziendale e disciplinando le condizioni per il corretto utilizzo degli strumenti informatici, telematici e telefonici da parte dei dipendenti della Provincia di Brescia e degli altri soggetti che vengono espressamente a ciò autorizzati.

L'utilizzo delle risorse informatiche e telematiche aziendali, in applicazione di quanto disposto dagli artt. 2104 e 2105 c.c., deve avvenire nell’ambito del generale contesto di diligenza, fedeltà e correttezza, adottando tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, anche in considerazione della difficoltà di tracciare una netta

linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e di terzi che interagiscono con quest'ultimo.

1.1 Destinatari

Le presenti "Linee guida" sono vincolanti per tutti gli *Utenti* (vedi art. 1.4 delle presenti "Linee guida") che, nell'espletamento dei propri compiti, utilizzano le reti e le risorse informatiche e/o telematiche della Provincia di Brescia: lavoratori dipendenti (senza distinzione di ruolo e/o livello), amministratori provinciali, collaboratori esterni (a progetto, stage, liberi professionisti, ecc.) e personale incaricato da operatori economici affidatari di servizi che prevedono accessi alle risorse informatiche della Provincia.

E' pertanto responsabilità di tutti i soggetti che utilizzano gli strumenti informatici messi a disposizione, di applicare e rispettare puntualmente le disposizioni delle presenti "Linee guida", ferme restando le disposizioni normative in materia, e tutte le prescrizioni previste per il trattamento dei dati sensibili o giudiziari.

Sono esentati dall'applicazione delle presenti "Linee guida", e limitatamente a quanto necessario per il corretto svolgimento delle proprie funzioni, gli Amministratori di Sistema.

1.2 Finalità

La Provincia di Brescia è ben consapevole che il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati.

Le presenti "Linee guida" intendono perciò precisare modi e forme con le quali, in una cornice di reciproci diritti e doveri, possa essere meglio assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali, da un lato, e il giusto perseguimento dei fini propri della Provincia, dall'altro.

Le "Linee guida" definiscono pertanto le policy predisposte e applicate dalla Provincia di Brescia relativamente all'utilizzo di alcuni strumenti elettronici nel contesto lavorativo; esplicita altresì i dati personali che sono o possono essere tracciati sui sistemi per effetto dell'utilizzo di alcuni strumenti elettronici; indica i possibili controlli leciti esercitabili dalla Provincia di Brescia circa l'effettivo utilizzo degli strumenti e il rispetto delle policy nonché, per i casi di eventuale violazione, le procedure e le sanzioni applicabili. Definisce, conformemente al diritto vigente, le policy predisposte e applicate dalla Provincia di Brescia in relazione all'utilizzo di Internet, e-mail, telefonia ed altri strumenti elettronici nel contesto lavorativo, nonché gli eventuali controlli e le relative sanzioni a carico dei lavoratori.

Le presenti "Linee guida" perseguono le seguenti finalità:

- definire le regole di utilizzo degli strumenti elettronici da parte degli utenti, così come definiti al successivo art. 1.4, con particolare riferimento a Internet, posta elettronica, postazioni di lavoro e di telefonia;
- informare gli utenti circa le modalità di trattamento dei dati personali che conseguono all'utilizzo degli strumenti elettronici;
- fornire agli utenti gli estremi identificativi delle persone fisiche che ricoprono il ruolo di amministratori di sistema e fissare obblighi e divieti in capo a questi ultimi;
- regolamentare, nel rispetto della normativa vigente, le modalità di controllo sul corretto utilizzo degli strumenti e sul rispetto delle regole, nonché stabilire, in caso di violazione, le procedure e le sanzioni applicabili.

Le regole contenute nelle presenti “Linee guida” sono fissate in conformità con i principi desumibili dalla normativa vigente in materia di protezione dei dati personali e dalle direttive del Garante, quali:

- garanzia del perseguimento dei fini istituzionali della Provincia;
- rispetto della libertà di espressione della personalità dell'Utente;
- ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali;
- prevenzione dei comportamenti scorretti o illeciti;
- garanzia della sicurezza e della disponibilità dei dati.

1.3 Quadro normativo

Costituiscono riferimenti normativi fondamentali delle presenti “Linee guida”:

- Art. 15 della Costituzione italiana
- Codice Civile, in particolare artt. 2087, 2104, 2105 e 2106
- Legge n. 300/1970 (Statuto dei lavoratori), in particolare gli artt. 4 e 8
- Provvedimento del Garante per la protezione dei dati personali n. 13 del 31/03/2007
- Provvedimento del Garante 27/11/08 sugli amministratori di sistema
- Direttiva n° 02/2009 del Dipartimento Funzione Pubblica
- Regolamento dell'Ente in materia di protezione dati personali
- Regolamento dell'Ente in materia di trattamento dei dati sensibili e giudiziari
- Regolamento dell'Ente sui sistemi e servizi informatici e telematici. (D.C.P. n° 62 del 20/12/2002)
- Art. 615 ter C.P. (accesso abusivo a sistema informatico)
- Codice dell'Amministrazione Digitale
- Giurisprudenza di Cassazione e di merito
- Normativa Trasparenza (L. 190/2012)
- Normativa Open Data (D.L. 22 giugno 2012, n. 83)
- GDPR – Regolamento UE 2016/679 e successivi provvedimenti attuativi
- Normativa sul diritto d’autore

1.4 Definizioni

Di seguito si fornisce l’elenco dei termini utilizzati dalle presenti “Linee guida” e le relative definizioni.

- **Utente**: soggetto a cui sono state assegnate delle credenziali di accesso e che utilizza le attrezzature informatiche, i servizi e/o gli strumenti del sistema informatico della Provincia di Brescia (può essere sia un dipendente che un collaboratore, che un amministratore, che un fornitore).
- **Dirigente del Settore Innovazione**: Dirigente del Settore Innovazione o il dirigente/posizione apicale che è responsabile del settore/servizio preposto alla gestione del “sistema informatico/informativo” dell’Ente.
- **Dirigente responsabile**: Dirigente del settore di appartenenza dell’Utente.
- **Dominio**: spazio virtuale, al quale vengono associate tutte le risorse di una infrastruttura di rete, al fine di renderle disponibili agli utenti dotati di credenziali di autenticazione al domino.
- **Accesso al Dominio**: procedura di autenticazione effettuata da un Utente mediante inserimento delle proprie credenziali di dominio (Username e Password).

- **Single Sign On (SSO)**: processo centralizzato di autenticazione, superato il quale è possibile accedere a una serie di servizi senza necessità di inserire nuovamente le proprie credenziali.
- **Amministratore di sistema**: la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione o di sue componenti e tutte le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati personali, quali gli amministratori di basi di dati, di reti informatiche, di apparati di sicurezza e di sistemi di software complessi, nella misura in cui consentano di intervenire sui dati personali; soggetti che, pur non essendo preposti ordinariamente a operazioni implicanti una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), possono, nelle loro consuete attività, essere concretamente responsabili di specifiche fasi lavorative comportanti elevate criticità rispetto alla protezione dei dati personali;
- **Cookies**: files di piccole dimensioni inviati dai server dei siti web visitati e salvati dai browser per tenere traccia delle informazioni sulla navigazione.
- **Indirizzo IP** (**Internet Protocol address**): è un'etichetta numerica che identifica un dispositivo detto host collegato a una rete informatica.
- **File (**traducibile dall'inglese come "archivio", ma comunemente chiamato anche "documento"): viene utilizzato per riferirsi a un contenitore di informazioni/dati in formato digitale.
- **Host**: indica ogni terminale collegato, attraverso link di comunicazione, ad una rete informatica (es. Internet).
- **DHCP** (Dinamic Host Configuration Protocol): servizio di rete che associa un dispositivo di rete ad un indirizzo IP mediante il quale poter comunicare con l'infrastruttura della rete stessa.
- **DNS** (Domain Name System): servizio di rete che associa un nome di un nodo della rete con unindirizzo IP.
- **NAT** (Network Address Translation): servizio che consente gestire le richieste e le risposte tra gli host di una rete privata e host su una rete pubblica.
- **Log:** tracce elettroniche relative all'utilizzo di strumenti elettronici da parte di un Utente o di un processo.
- **BIOS (**Basic Input Output System): rudimentale insieme di routine di software che consente di configurare ed eseguire la procedura di avvio di un computer.
- **Malware**: un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito e/o alla rete di computer alla quale il nodo infetto è connesso. Appartengono alla categoria: virus, worm, trojan, rootkit, keylogger, ecc.
- **Backup:** procedura con la quale si realizza una copia di sicurezza (detta anch'essa backup o copia di backup) di un certo insieme di dati:
- **Disaster recovery:** insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi dell'ente, associazione o impresa, a fronte di gravi emergenze che ne intacchino la regolare attività.
- LAN: acronimo del termine inglese Local Area Network, in italiano rete locale. Identifica una rete costituita da computer collegati tra loro, dalle interconnessioni e dalle periferiche condivise in un ambito fisico delimitato (esempi: una stanza, un edificio, più edifici vicini).
- Policy: Insieme delle misure organizzative e dei comportamenti che devono essere tenuti dai dipendenti, collaboratori ed amministratori per contrastare i rischi informatici.

- Alias: un alias di posta è un Utente virtuale che non ha in realtà una casella propria: riceve le mail ma automaticamente queste vanno a finire nella casella dell'Utente reale di cui è alias: in pratica si tratta di un reindirizzamento. Quindi le e-mail indirizzate alla casella postale dell'alias sono convogliate su un'unica casella reale per essere ritirate

1.5 Informativa resa all'Utente

Con le presenti "Linee guida" la Provincia, in qualità di titolare del trattamento dati, intende adempiere all'onere, previsto dal Regolamento Europeo 2016/679, di informare gli utenti circa le forme e le modalità di trattamento dei loro dati personali, che derivano dall'utilizzo di strumenti elettronici.

Mediante lettura delle presenti "Linee guida", ogni Utente viene reso edotto del fatto che esistono procedure automatiche di monitoraggio delle attività, effettuate per ragioni di sicurezza dai dispositivi dell'infrastruttura di rete, che possono indirettamente dare luogo a "trattamenti" di dati personali dell'Utente o di terzi. Le caratteristiche dei trattamenti in questione saranno descritte nei successivi articoli delle "Linee guida".

In merito a tali trattamenti, gli interessati possono esercitare i diritti di cui agli articoli 7, 8 e 9 del D. Lgs. 196/03 rivolgendosi al Dirigente del Settore Innovazione della Provincia di Brescia.

1.6 Modalità di pubblicizzazione delle presenti "Linee guida"

1.6.1 Utenti interni

Le presenti "Linee guida" e i relativi allegati vengono resi disponibili in un'apposita sezione della Intranet provinciale al fine di darne massima diffusione.

1.6.2 Fornitori esterni

Qualora vengano assegnate ad un fornitore esterno risorse o attrezzature informatiche di proprietà della Provincia, oppure credenziali di accesso al dominio o a singoli host dell'infrastruttura di rete, spetta al Dirigente responsabile il compito di comunicare ai soggetti interessati queste "Linee guida" in formato digitale o cartaceo.

1.7 Aggiornamento periodico

Le presenti linee guida possono essere soggette ad aggiornamenti periodici, in considerazione di:

- modifiche e/o innovazioni di carattere tecnico-informatico;
- modifiche di carattere normativo;
- esperienze maturate, nel periodo di riferimento, in applicazione delle "Linee guida";
- nuove esigenze di sicurezza, produzione, organizzazione che abbiano impatto sugli aspetti trattati dalle "Linee guida".

Deroghe o modifiche di uno o più punti delle presenti "Linee guida" non rendono invalidi gli altri punti.

Gli aggiornamenti verranno pubblicizzati secondo quanto previsto all'art. 1.6.1 e all'art. 1.6.2.

1.8 Interpretazione delle presenti “Linee guida” e proposte di integrazione

Per qualsiasi dubbio relativo all’applicazione pratica o all’interpretazione delle disposizioni contenute nelle presenti linee guida, è possibile rivolgersi al personale del Settore che gestisce il “sistema informatico/informativo” inoltrando una segnalazione tramite email all’indirizzo di posta elettronica segreteria_informatica@provincia.brescia.it.

Art. 2. ORGANIZZAZIONE

2.1 Titolarità

La Provincia di Brescia è titolare di tutte le risorse hardware e software messe a disposizione degli utenti.

Tutto l'hardware e il software in dotazione ai Settori deve essere acquisito in accordo con le specifiche tecniche fornite dal Settore che gestisce il "sistema informatico/informativo" dell'Ente.

Tutte le risorse informatiche assegnate devono essere custodite con cura evitando ogni possibile forma di danneggiamento. Gli utenti sono responsabili del corretto utilizzo degli strumenti messi loro a disposizione e della loro custodia e sono tenuti a segnalare tempestivamente al Settore che gestisce il "sistema informatico/informativo" dell'Ente, eventuali guasti e/o furti nonchè difetti di funzionamento, anche di lieve entità, dei dispositivi hardware e software che possano pregiudicare il normale esercizio dell'attività lavorativa.

2.2 Uso tollerato per fini personali degli strumenti elettronici – Criteri generali

Nel convenire che internet e posta elettronica fanno ormai parte della vita quotidiana e che sempre più servizi vengono gestiti con la modalità on-line, la Provincia di Brescia riconosce la possibilità ai destinatari delle presenti "Linee guida" di utilizzare le dotazioni aziendali assegnate, in modo sporadico, anche per fini personali, purché nel rispetto delle prescrizioni sotto indicate:

- deve essere effettuato nel rispetto della Legge;
- deve rispettare le ulteriori regole e limiti stabiliti dalle presenti "Linee guida";
- deve essere attuato fuori dall'orario di lavoro (ad esempio durante la pausa pranzo), salvo casi di urgenza;
- non deve entrare in conflitto, ostacolare o impedire il corretto svolgimento delle prestazioni lavorative proprie o altrui, né avere impatto negativo sulle prestazioni dell'infrastruttura di rete;
- non deve arrecare costi aggiuntivi all'Ente. Eventuali costi sostenuti andranno rimborsati all'Ente secondo le modalità definite dal Settore che gestisce il "sistema informatico/informativo" dell'Ente e/o dall'Ufficio Stipendi.

Tutte le attività sopra indicate dovranno ispirarsi ai principi di buona fede contrattuale, non dovranno superare la soglia della ragionevolezza nè procurare danni alle dotazioni aziendali.

L'Utente risponderà di eventuali danni arrecati o di un uso ingiustificatamente esteso delle citate attività.

2.3 Elenco degli amministratori di sistema

Gli estremi identificativi degli amministratori di sistema possono essere richiesti tramite email all'indirizzo segreteria_informatica@provincia.brescia.it.

Gli amministratori di sistema possono accedere a tutte le risorse di rete, per finalità non eccedenti alle proprie mansioni e incarichi, secondo quanto previsto dalla sopra citata direttiva del Garante.

2.4 Valutazione impatto sull'ambiente lavorativo di eventuali nuovi strumenti

In caso di adozione o installazione di nuovi strumenti informatici che effettuano la raccolta o la conservazione di dati, mediante i quali sia possibile operare un controllo indiretto sulle attività svolte dagli Utenti, la Provincia di Brescia procede ad una valutazione dell'impatto sull'ambiente lavorativo e sui diritti degli Utenti.

La valutazione è predisposta dal Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente di propria iniziativa o su richiesta di altro Dirigente del trattamento ovvero su richiesta del Segretario Generale. L'esito della valutazione è contenuto in un documento sintesi, che contiene almeno:

- le caratteristiche del nuovo strumento che si intende installare;
- le ragioni che impongono o suggeriscono l'installazione, e le finalità perseguite;
- i tipi di dati che saranno raccolti a seguito dell'installazione del nuovo strumento;
- le misure eventualmente necessarie per mitigare l'impatto sui diritti degli utenti.

Il documento verrà utilizzato in sede di aggiornamento periodico delle presenti "Linee guida".

2.5 Competenze e responsabilità

Il Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente è tenuto a:

- elaborare le regole per un utilizzo ragionevolmente sicuro del sistema informativo della Provincia di Brescia;
- implementare, con l'ausilio del personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente, le regole di sicurezza sul sistema informativo dell'Ente;
- monitorare, con l'ausilio di personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente, e/o di personale incaricato interno/esterno, i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
- segnalare prontamente ai Dirigenti di Settore/Servizio ogni eventuale attività non autorizzata sul sistema informativo dell'Ente;
- attenersi alle prescrizioni previste nel "Documento di adozione delle misure e accorgimenti prescritti dal Garante per la Protezione dei Dati Personali ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- mantenere aggiornate le presenti "Linee Guida".

I Dirigenti responsabili dei vari settori/servizi sono tenuti a:

- informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo della Provincia;
- assicurare che il personale a loro assegnato si uniformi alle regole e alle procedure descritte nelle presenti "Linee guida";
- assicurare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nelle presenti "Linee guida";
- richiedere l'attivazione di nuove abilitazioni, di nuove caselle di posta elettronica e liste di distribuzione;
- controllare periodicamente che le abilitazioni in uso presso il settore/servizio e richiedere la disabilitazione di quegli accessi non più necessari;
- verificare che non esistano liste di distribuzione o numeri di fax server inutilizzate o che comunque non vengano presidiate da alcuno;
- richiedere la dotazione di nuove attrezzature;
- verificare che non esistano attrezzature non utilizzate o comunque non assegnate ad alcuno. In tal caso deve provvedere alla loro restituzione al Settore che gestisce il "sistema informatico/informativo" dell'Ente;

- verificare che non vengano collegate alla rete aziendale attrezzature non fornite e/o preventivamente configurate dal Settore che gestisce il "sistema informatico/informativo";
- verificare che le attrezzature fornite non vengano manomesse e/o non vengano utilizzate con periferiche non autorizzate (ad esempio chiavette per la navigazione, router, ecc.);
- adempiere a tutti gli obblighi inerenti la responsabilità loro affidata in materia di trattamento di dati personali e sensibili gestiti dalla Provincia;
- segnalare prontamente al Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente, ogni eventuale attività non autorizzata sul sistema informativo dell'Ente.

Il personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente e l'eventuale personale esterno incaricato che concorre alla gestione/implementazione del sistema informativo della Provincia è tenuto a:

- garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
- segnalare prontamente al Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente, ogni eventuale attività non autorizzata sul sistema informativo dell'Ente.

Tutti gli Utenti del sistema informativo sono responsabili per ciò che concerne:

- il rispetto delle presenti "Linee Guida" e delle normative in essere;
- l'uso delle credenziali di autenticazione loro assegnate secondo le modalità previste nelle presenti "Linee guida";
- la pronta segnalazione al Dirigente responsabile in merito a ogni eventuale attività non autorizzata sul sistema informativo dell'Ente di cui vengano a conoscenza.

2.6 Richiesta servizi

Tutte le richieste di attivazione servizi e di fornitura attrezzature dovranno essere inoltrate al Settore che gestisce il "sistema informatico/informativo" dell'Ente, secondo le modalità rese disponibili sulla intranet aziendale.

Il Dirigente responsabile potrà anche richiedere al Settore che gestisce il "sistema informatico/informativo" dell'Ente, la rendicontazione dei servizi attivi e degli asset assegnati al proprio settore.

Il Settore che gestisce il "sistema informatico/informativo" dell'Ente, mette a disposizione degli utenti un servizio di helpdesk per la gestione delle richieste di assistenza tecnica informatica. Le modalità di attivazione sono pubblicate sulla intranet aziendale.

2.7 Acquisizione - sviluppo nuovi applicativi

In caso di acquisizione e/o sviluppo di nuovi applicativi da parte degli uffici interni all'Ente, anche se commissionati a soggetti terzi, il dirigente del settore di riferimento deve rendere disponibile al dirigente che gestisce il "sistema informatico/informativo" dell'Ente:

- l'accesso al codice sorgente e alle base dati;
- l'analisi e la documentazione sul funzionamento e l'installazione;
- i metadati sulle strutture dati, eventualmente implementate.

La proprietà di quanto sopra, inclusi i diritti derivanti, sono dell'Ente salvo il diritto di essere riconosciuto autore dell'invenzione [Titolo IX del Libro Quinto del Codice Civile, D. Lgs. 518 del 29 dicembre 1992 che novella la legge 633/41].

2.8 Proprietà intellettuale e delle licenze d'uso

Tutto il software in uso nel sistema informativo dell'Ente, in cui sia prevista una licenza d'uso, deve essere registrato a nome di Provincia di Brescia.

Il software può essere individuato dal settore competente in materia, anche su suggerimento da parte del Settore che gestisce il "sistema informatico/informativo" dell'Ente.

Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza.

Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale, sia per quanto riguarda il software che per quanto riguarda i file di qualsiasi altra natura (ad esempio video).

2.9 Attività svolte ai fini dell'assistenza tecnica agli utenti

Ai soli fini di prestare assistenza tecnica informatica, la Provincia di Brescia utilizza uno o più software che permettono di assumere il controllo remoto di un PC all'interno della sessione di lavoro dell'Utente. L'attivazione del collegamento al PC dell'Utente può essere richiesta unicamente da un tecnico che deve essere stato incaricato dal Settore che gestisce il "sistema informatico/informativo" dell'Ente (operatori di helpdesk, fornitori di applicativi, amministratori di sistema, ecc.) e deve essere finalizzata allo svolgimento dell'attività di assistenza tecnica informatica.

La sessione remota è subordinata al preventivo consenso da parte dell'Utente, al quale verrà comunicato il termine dell'attività stessa. In nessun caso è autorizzato l'ingresso in una sessione di lavoro da parte di un amministratore di sistema o operatore di helpdesk senza il preventivo consenso dell'Utente.

Nell'0 delle presenti "Linee guida" sono elencati gli strumenti software utilizzati dagli amministratori di sistema/operatori di helpdesk per svolgere l'attività di assistenza tecnica remota, nonché i nominativi dei fornitori esterni autorizzati a richiedere agli utenti l'accesso remoto ai sistemi informatici.

E' tassativamente vietato agli utenti comunicare a soggetti diversi da quelli autorizzati a svolgere assistenza tecnica le credenziali di accesso ai software di assistenza remota.

In ogni caso, l'Utente è tenuto presidiare la propria postazione durante l'intera sessione di connessione da remoto.

Se, nell'ambito dell'attività manutentiva, anche in telediagnosi, verrà riscontrato l'utilizzo di programmi, files, etc. non previsti e/o non afferenti l'attività lavorativa o comunque non autorizzati dal Settore che gestisce il "sistema informatico/informativo" il tecnico provvederà all'eliminazione di tali files e/o alla disinstallazione dei software, e/o alla segnalazione dell'attività svolta o di quanto riscontrato al Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente. Lo stesso vale per qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.

A seguito della segnalazione inoltrata dal tecnico, il Responsabile del Settore che gestisce il "sistema informatico/informativo" dell'Ente dovrà inoltrare apposita segnalazione o contattare direttamente il Settore Personale o il Dirigente responsabile dell'Utente assegnatario della postazione.

Non verrà fornita assistenza sulle attrezzature, sui sistemi operativi e sugli applicativi non forniti dal Settore che gestisce il "sistema informatico/informativo" dell'Ente.

Art. 3. DISPOSIZIONI SULL'UTILIZZO DELLE DOTAZIONI INFORMATICHE

3.1 Gestione ed assegnazione delle credenziali di autenticazione al dominio e alle risorse di rete

Le risorse dell'infrastruttura di rete della Provincia di Brescia sono organizzate in uno spazio virtuale definito "dominio". Per l'accesso al dominio viene rilasciata una credenziale di autenticazione composta da un codice di identificazione (user name o user id) associato ad una parola chiave riservata (password). Tale credenziale viene rilasciata a tutti i dipendenti e amministratori, mentre per i collaboratori e i fornitori viene rilasciata solo su richiesta del Dirigente responsabile. Tale credenziale può consentire, se abilitata, anche l'accesso alla rete aziendale, alla casella di posta elettronica nominativa e alla intranet, oltre che ad alcuni applicativi gestionali (se l'accesso è previsto tramite SSO).

La credenziale di autenticazione consiste in un codice univoco per l'identificazione dell'Utente (user name), assegnato dal Settore Innovazione, associato ad una parola chiave (password) riservata che dovrà essere custodita dall'Utente con la massima diligenza e non divulgata.

Per meglio gestire le credenziali si consiglia all'Utente di attenersi alle seguenti regole:

- la password deve essere sostituita in occasione del primo accesso al dominio e successivamente almeno ogni tre mesi;
- la parola chiave deve essere composta da almeno otto caratteri alfanumerici (facendo attenzione alla differenza tra caratteri minuscoli e maiuscoli) e deve contenere almeno un numero, inoltre non può essere uguale alle ultime due utilizzate;
- la parola chiave deve formare un codice non banale che non abbia alcun riferimento con dati personali (user name, nome, cognome, indirizzo, data di nascita, ecc.) dell'Utente, di parenti, amici, colleghi o conoscenti;
- la parola chiave deve essere mantenuta segreta e non deve essere rivelata ad alcuno. Se conservata in forma scritta deve essere custodita con diligenza in un luogo accessibile soltanto all'Utente (preservata dalla conoscibilità di colleghi o soggetti esterni all'ente);
- in nessun caso devono essere annotate password in chiaro, sia su supporto cartaceo che informatico;
- per la modifica della password, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, procedere secondo quanto dettagliato all'allegato B;
- durante la digitazione della propria password, assicurarsi che nessuno stia osservando la tastiera con l'intenzione di memorizzarla;
- qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione al proprio Dirigente.

Superata la procedura di autenticazione, l'Utente può accedere al proprio pc e, sulla base delle autorizzazioni che gli sono state rilasciate, operare sulle cartelle di rete, utilizzare gli applicativi, navigare su Internet e consultare la posta elettronica. L'accesso alle postazioni di lavoro sarà effettuato con privilegio di Utente non amministratore, salvo specifica autorizzazione rilasciata dal Settore che gestisce il "sistema informatico/informativo" dell'Ente.

3.2 Accessi non nominativi

Gli accessi non nominativi (ad esempio per i fornitori che devono fare assistenza sul server da remoto) possono essere richiesti solamente in casi eccezionali in quanto la regola presuppone che gli accessi siano nominativi.

Nel caso in cui debbano essere richiesti deve essere fatta una "Richiesta dirigenziale" nella quale oltre a motivarne la necessità e i dettagli tecnici deve indicare chi è il responsabile di tale accesso.

Il direttore del Settore che gestisce il "sistema informatico/informativo" si riserva di valutarne l'eventuale creazione.

3.3 Certificati digitali: (es.: Firma digitale, CRS)

Il certificato digitale è nominativo e strettamente personale. Occorre provvedere all'installazione del certificato digitale sul proprio "profilo" onde evitare che la propria identità venga utilizzata da parte di Terzi per l'accesso e la registrazione su procedure informatiche.
In caso di utilizzo di certificati digitali su postazioni di lavoro condivise, ove consentito, occorre attivarne la protezione mediante l'impostazione della password con le caratteristiche di "robustezza" sopra indicate.
L'Utente si impegna a comunicare quanto prima al Settore che gestisce il "sistema informatico/informativo" dell'Ente, l'eventuale furto o smarrimento del proprio certificato digitale.

3.4 Rete

In assenza di specifica autorizzazione da parte del Settore che gestisce il "sistema informatico/informativo" dell'Ente, non è consentito accedere ai locali tecnici e ai box riservati alle apparecchiature di rete.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Settore che gestisce il "sistema informatico/informativo" dell'Ente (quali ad esempio hub, switch, access point o altre componenti personali).

Non è consentito installare o utilizzare qualsiasi altra apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Settore che gestisce il "sistema informatico/informativo" dell'Ente, quali, a titolo esemplificativo: modem, router, Internet key, ecc.

Non è consentito effettuare spostamenti o modifiche di risorse collegate alla rete aziendale (es.: pc, stampanti, multifunzione e altro) senza una preventiva autorizzazione da parte del Settore che gestisce il "sistema informatico/informativo" dell'Ente.

Quanto detto vale sia per la rete fisica (cavo) che quella wireless (reti wi-fi)

3.5 Utilizzo delle condivisioni di rete

Per l'accesso alla rete della Provincia ciascun Utente deve essere in possesso della specifica credenziale di autenticazione (vedi art. 3.1). È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione Utente diverso da quello assegnato.

Gli spazi delle unità di rete messi a disposizione, sono aree di condivisione e di archiviazione di informazioni strettamente lavorative e non possono pertanto essere utilizzate per la memorizzazione di file non attinenti ad attività lavorative. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

In queste aree dovranno essere necessariamente salvati tutti i documenti lavorativi afferenti al Settore-Ufficio di appartenenza, al fine di renderli disponibili, in caso di necessità, ai colleghi.

Su queste unità vengono svolte regolari attività di controllo statistico, amministrazione, backup e restore da parte del personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente. Il personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza della rete.

Gli accessi nelle unità di rete condivise devono essere autorizzati da parte del Dirigente responsabile, il quale provvederà a richiedere al Settore che gestisce il "sistema informatico/informativo" dell'Ente, la creazione/rimozione dei diritti di accesso e a effettuare periodicamente la verifica delle abilitazioni attive.

Possono essere fornite ulteriori aree deputate allo scambio di file tra uffici diversi (es.: cartella "common", file scannerizzati da scanner di rete). Onde evitare la saturazione di questi spazi, cessato lo scopo contingente, i file salvati nelle aree comuni dovranno essere rimossi a cura dell'Utente che li ha memorizzati, diversamente, verranno rimossi mediante la programmazione di apposite procedure di cancellazione automatica con la frequenza che verrà resa nota sulla intranet.

In aggiunta alle cartelle condivise, la Provincia di Brescia fornisce ad ogni Utente una cartella ad accesso nominativo (home directory) identificata con l'unità disco U, al fine di poter archiviare documenti concernenti la propria vita lavorativa (ad esempio documenti, manuali, appunti, ecc.) e per i quali non è dovuta la condivisione del contenuto con altri utenti. Le "home directory" restano valide per tutta la durata della permanenza in servizio dello stesso Utente titolare; hanno una dimensione predefinita e non estendibile. Le specifiche tecniche di tali cartelle (dimensione, modalità di utilizzo, ecc.) saranno rese disponibili sulla intranet.

In nessuna risorsa di rete è consentito salvare file audio, video, eseguibili e archivi di posta elettronica ad eccezione di quelli strettamente attinenti a esigenze lavorative e su specifica autorizzazione da parte del Dirigente responsabile.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun Utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione inoltre deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

3.6 Utilizzo del PC (Personal Computer) – Postazione fissa

Il Personal Computer affidato all'Utente è uno strumento di lavoro il cui utilizzo a fini personali è vietato se non nei limiti specificati nell'art. 2.2. Ogni utilizzo non inerente all'attività lavorativa, che superi tali limiti è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Gli utenti, nell'utilizzo degli strumenti informatici assegnati, devono evitare comportamenti che possono anche solo potenzialmente recare danno alle strumentazioni ed alle banche dati.

Il PC dato in affidamento all'Utente permette l'accesso alla rete della Provincia di Brescia solo attraverso specifiche credenziali di autenticazione come meglio descritto all'art. 3.1 delle presenti "Linee guida".

Ogni Utente che accede ad un personal computer è pienamente responsabile di tutte le azioni che compie sulla rete aziendale. I permessi di accesso alle risorse di rete sono concessi a ciascun Utente (lettura, scrittura, cancellazione e recupero dei dati) dall'Amministratore di Sistema, coerentemente con quanto richiesto dal proprio Dirigente responsabile. Qualora venissero effettuate ed individuate indebite azioni di creazione, cancellazione o modifica dei dati, l'Amministratore di Sistema dovrà inoltrare apposita segnalazione al dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente, per eventuali provvedimenti.

Gli Amministratori di sistema sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché ad eseguire, interventi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.). Per l'esecuzione di detti interventi potrebbe essere necessario anche l'accesso ai dati di ciascun Utente (ad esempio: documenti salvati sui dischi di rete e/o sul PC, archivio di posta elettronica, log di navigazione, ecc.).

Il personale incaricato del Settore che gestisce il "sistema informatico/informativo" dell'Ente, ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato secondo le modalità indicate all'art. 2.9 ed avviene su richiesta dell'Utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Il PC viene assegnato con la configurazione standard predefinita dal Settore che gestisce il "sistema informatico/informativo" dell'Ente:

- l'Utente deve custodire l'attrezzatura con la massima cura (vedi art. 5.1);
- l'Utente non deve modificare le impostazioni autonomamente;
- è vietato modificare le policy impostate dall'Amministratore di Sistema (ad esempio interrompendo gli aggiornamenti automatici dei sistemi);
- è vietato effettuare sulle apparecchiature operazioni di formattazione dell'hard disk o reset degli apparati;
- l'Utente è tenuto a bloccare l'accesso ai propri dispositivi qualora dovesse lasciarli incustoditi anche per un breve lasso di tempo. Ad esempio nel caso in cui si dovesse assentare dall'ufficio il proprio personal computer andrà spento o quanto meno bloccato effettuando il logoff (disconnetti) dell'Utente o il "blocca computer"; in ogni caso tutti i programmi e documenti dovranno essere chiusi;
- non è consentito aprire, visualizzare o copiare file provenienti da supporti esterni se non inerenti l'attività lavorativa o se non espressamente autorizzati dal proprio Dirigente, fermo restando il fatto che resta a carico dell'Utente la preliminare scansione antivirus;
- non è consentito modificare per nessun motivo la configurazione hardware o software dei personal computer o degli altri strumenti informatici o elettronici se non espressamente autorizzati dal proprio Dirigente.
- non è consentita l'installazione sul proprio PC di mezzi di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem e dispositivi bluetooth, ecc.), salvo l'autorizzazione espressa del Dirigente responsabile;
- non verranno forniti privilegi di "amministratore" a eccezione di specifiche e motivate esigenze – vedi art. 3.12;
- è vietato l'utilizzo di cd rom anche riscrivibili, dvd, USB key, hard disk esterni, unità di memoria di massa esterne o altro dispositivo di memorizzazione di provenienza ignota e/o personali;
- è fatto divieto assoluto di memorizzare e conservare documenti, files o dati ottenuti in modo illegale (ad esempio software soggetti a copyright, file musicali soggetti a copyright, file video soggetti a copyright, ecc.);
- il PC deve essere spento al termine dell'orario di lavoro. In caso di assenze prolungate (compresa la sosta pranzo) o in caso di suo inutilizzo il pc dovrà essere spento ovvero disconnesso (vedi 0), in maniera tale che al primo accesso il sistema chieda l'inserimento di login e password dell'assegnatario. In ogni caso,

lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso**;**

- non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito utilizzare strumenti potenzialmente in grado di consentire accessi non autorizzati alle risorse informatiche (es.: programmi di condivisione quali IRC, ICQ, AudioGalaxy o software di monitoraggio della rete in genere);
- non è consentito configurare o utilizzare servizi diversi da quelli messi a disposizione da parte del Settore Innovazione (quali DNS, DHCP, server internet (Web, FTP,…);
- non è consentito intercettare pacchetti sulla rete (sniffer) o software dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'Utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali;
- non è consentito disassemblare il computer, asportare, scollegare, aggiungere, spostare o semplicemente scambiare tra un PC e l'altro qualsiasi componente e/o periferica in dotazione all'Utente;
- non è consentito avviare il personal computer con sistemi operativi diversi da quello installato dal Settore Innovazione, incluse versioni live;
- è vietato avviare i personal computer utilizzando dispositivi di boot differenti (ad esempio live cd, usb drives, ecc.) rispetto a quelli predefiniti;
- è fatto divieto di accedere alla configurazione BIOS dei singoli personal computer, e tantomeno è loro consentito di modificare tale configurazione o impostare password di protezione per l'accesso al sistema o al BIOS;
- sono vietati l'installazione e l'utilizzo di interfacce di rete o dispositivi di connessione di rete diversi da quelli preconfigurati dal Settore che gestisce il "sistema informatico/informativo" dell'Ente. Per i computer dotati di scheda di rete wireless, è vietato connettersi a reti wi-fi diverse da quelle messe a disposizione dalla Provincia di Brescia;
- è vietato connettere alla rete LAN provinciale computer o altri dispositivi personali senza l'autorizzazione del Settore che gestisce il "sistema informatico/informativo" dell'Ente. Tale autorizzazione deve essere richiesta in forma scritta dal Dirigente responsabile. In ogni caso, i dispositivi personali autorizzati dovranno assicurare il rispetto delle misure minime di sicurezza, ovvero la presenza di un software antivirus attivo ed aggiornato;
- non è consentito utilizzare connessioni in remoto per l'accesso a risorse, al di fuori del perimetro aziendale e fatte salve le connessioni realizzate e autorizzate da parte del Settore che gestisce il "sistema informatico/informativo" dell'Ente;
- ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Settore Innovazione nel caso in cui siano rilevati virus ed adottando quanto previsto dall'art. 3.10 delle presenti "Linee guida", relativo alle procedure di protezione antivirus;
- files memorizzati nel PC vanno salvati esclusivamente nel "profilo Utente" e cioè nella cartella documenti o sul desktop (e/o in eventuali loro sotto cartelle). Si rammenta che tutte le cartelle del disco C sono gestite dall'amministratore di sistema che ne potrà disporre a seconda delle esigenze e delle politiche di gestione definite (ad esempio la cartella Programmi verrà utilizzata solo per l'installazione degli applicativi, eventuali cartelle sconosciute potrebbero essere rimosse, ecc.). Eventuali altri dischi del PC (ad esempio d:, e:) devono essere lasciati liberi in quanto potrebbero servire all'amministratore di

sistema per il ripristino del sistema operativo. Si sottolinea che non esistono automatismi per il backup dei dati Utente pertanto, in caso di guasto hardware del PC, potrebbero non essere recuperabili;

- è vietato impostare condivisioni di cartelle e/o di file;
- è vietato stampare o fotocopiare documenti personali utilizzando le stampanti/fotocopiatrici multifunzione aziendali.

Si rammenta che i dischi o le altre unità di memorizzazione locale (ad esempio disco C:) non devono essere utilizzate per salvare documenti frutto dell'attività lavorativa e quindi non sono soggette a backup da parte del personale incaricato del Settore che gestisce il "sistema informatico/informativo" dell'Ente. La responsabilità del salvataggio e dell'integrità dei dati ivi contenuti è pertanto a carico del singolo Utente.

Si sottolinea l'importanza del rispetto di quanto sopra elencato, in ragione del fatto che tali attività potrebbero invalidare le policy di sicurezza e mettere a repentaglio l'integrità dell'intera infrastruttura di rete della Provincia di Brescia.

Se nel corso delle attività di manutenzione ordinaria dei sistemi informativi si riscontrasse un utilizzo improprio di un dispositivo, ai fini di tutela del patrimonio aziendale o comunque nell'ambito della correttezza delle relazioni intercorrenti tra datore di lavoro e dipendenti, il Dirigente che gestisce il "sistema informatico/informativo" dell'Ente darà preventivo avviso generalizzato o circoscritto agli utenti afferenti il Settore in cui e stato rilevato il comportamento anomalo, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite; contrariamente, in caso di reiterazione, potrà previa comunicazione al trasgressore, ritirare il dispositivo ovvero eseguire tutti i controlli ritenuti necessari presso la postazione interessata, compresa la copia dei dati, programmi, files immagazzinati nella memoria interna del PC. Di dette attività dovrà essere data informazione al Settore Personale per ogni procedura e/o procedimento inerente. I dati raccolti con le modalità sopra indicate, saranno conservati dal datore di lavoro per il periodo strettamente necessario alla definizione, eventualmente anche in sede contenziosa, di ogni procedura e/o procedimento inerente. Al termine saranno cancellati e/o restituiti al trasgressore nel rispetto della vigente normativa sulla protezione dei dati.

3.6.1 Software

Onde evitare problemi di malfunzionamento, sicurezza e instabilità dei sistemi il computer viene fornito con configurazione software predefinita che non può essere per alcun motivo modificata da parte dell'Utente.

Nel caso in cui si ritenesse di avere necessità di un software / utility / programma non installato sul PC in dotazione, il Dirigente responsabile ne potrà far richiesta al Settore che gestisce il "sistema informatico/informativo" dell'Ente, che ne valuterà la compatibilità con l'infrastruttura esistente e provvederà all'eventuale installazione.

Il sistema operativo e tutti i moduli e programmi software messi a disposizione devono essere utilizzati esclusivamente per attività professionali; al contrario non possono essere utilizzati per attività profittevoli, e non possono essere copiati e distribuiti su installazioni esterne.

E' fatto divieto assoluto di utilizzo e/o possesso di software illegalmente copiato o comunque privo di regolare licenza d'uso, diverso da quelli ufficialmente installato dal personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente, per conto della Provincia di Brescia. Non è consentito agli Utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. Per lo stesso motivo non è consentito cambiare le configurazioni hardware e software impostate dall'Amministratore di Sistema e salvare files non aventi attinenza con la propria attività lavorativa che per dimensione e/o contenuto siano palesemente in contrasto con la funzione che la dotazione informatica assegnata è chiamata a svolgere. L'inosservanza della presente disposizione espone la stessa Provincia a gravi responsabilità anche

penali; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore (si vedano il D.Lgs 29.12.19992, n. 518 "Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore" e la L. 18.08.2000, n. 248 "Nuove norme di tutela del diritto di autore") sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente;

L'Utente deve verificare che tutti i software standard (di cui all'Allegato C) siano correttamente installati e funzionanti sulla postazione in uso; in caso contrario, dovrà aprire una richiesta di assistenza al servizio di Helpdesk per richiederne la corretta installazione e configurazione (vedi art. 2.6).

3.7 Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun Utente dovrà contattare il personale del Settore che gestisce il "sistema informatico/informativo" dell'Ente e seguire le istruzioni da questo impartite.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi in armadi chiusi. A tal proposito si ricorda che l'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Nel caso di utilizzo condiviso dei medesimi supporti da parte di più Utenti, occorre provvedere alla cancellazione delle informazioni ivi contenute mediante programmi formattazioni a basso livello.

Nel caso di smaltimento, i supporti dovranno essere precedentemente distrutti mediante punzonatura o deformazione meccanica o distruzione fisica o demagnetizzazione.

3.8 Utilizzo di postazioni condivise

Nel caso in cui la postazione di lavoro debba essere condivisa, ciascun Utente che accede al computer non potrà avere un profilo di amministratore locale.

3.9 Utilizzo di PC portatili

L'Utente è responsabile delle attrezzature assegnategli e deve custodirle con diligenza, sia durante gli spostamenti sia durante l'utilizzo, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

Ai PC portatili (ad es. notebook, netbook, ecc.) si applicano le regole di utilizzo previste dalle presenti "Linee guida" per le postazioni fisse (art. 3.6), con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

Le attrezzature utilizzate in occasione di eventi/attività esterne (convegni, fiere, etc.), in caso di allontanamento temporaneo dell'assegnatario, dovranno essere custoditi in luogo protetto.

3.10 Software antivirus e antimalware

Il sistema informatico della Provincia di Brescia è protetto da software antivirus aggiornato quotidianamente. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

E' buona norma controllare il regolare funzionamento e l'aggiornamento periodico del software installato secondo le procedure previste – Vedi Allegato D.

Ogni dispositivo magnetico di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Settore Innovazione.

Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale del Settore Innovazione.

Durante la navigazione web e l'utilizzo della posta elettronica è possibile che gli strumenti informatici in uso agli utenti vengano a contatto con virus e malware in generale. Per prevenire questo fenomeno, il Settore che gestisce il "sistema informatico/informativo" dell'Ente, provvede ad installare, configurare e gestire uno o più software antivirus (sia in locale sui PC sia sui server) in grado di proteggere l'infrastruttura dalle potenziali minacce. Tali software analizzano in modo automatico i file che l'Utente scarica attraverso la navigazione in internet o come allegati alla posta elettronica, rilevano i file infetti e tentano di renderli inoffensivi. Si sottolinea che nessuno dei software antivirus in commercio è in grado di individuare la totalità dei malware circolanti, per cui è di fondamentale importanza il fatto che tutti gli utenti dell'infrastruttura di rete tengano un comportamento responsabile ed evitino di scaricare/caricare files di provenienza non nota o da/su siti web o tramite la posta elettronica. Le istruzioni pratiche relative all'utilizzo del software antivirus sono contenute nell'Allegato D alle presenti "Linee guida".

3.11 Utilizzo delle stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:

- stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
- prediligere le stampanti di rete o multifunzione in luogo di quelle locali, al fine di ridurre l'utilizzo di materiali di consumo (toner, cartucce, ecc.);
- prediligere le stampanti laser in luogo di quelle che prevedono consumi maggiori, quali ad esempio le stampanti a getto di inchiostro;
- stampare laddove possibile la stampa in bianco/nero e in fronte/retro, al fine di ridurre i costi;

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà aver cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

3.12 Privilegi di amministratore locale

Su specifica e motivata esigenza, rappresentata dal Dirigente responsabile, possono essere concessi a particolari Utenti i privilegi di amministrazione locale della propria postazione di lavoro. Tali utenti saranno tenuti ad adottare le misure minime per mantenere inalterati gli attuali livelli di sicurezza informatica dei sistemi interessati e della rete aziendale.

3.13 Modalità di memorizzazione di documenti sui sistemi provinciali

Per il salvataggio dei dati, l'uso delle unità di rete e dei supporti di memorizzazione, oltre a quanto riportato nelle presenti "Linee guida", l'Utente si deve attenere alle seguenti regole:

- le unità di rete sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi; pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
- è da evitare il salvataggio dei propri dati sui singoli personal computer; i dati inerenti l'attività lavorativa devono essere salvati sulle unità di rete predisposte (server) che potrebbero essere accessibili (condivise) da altri utenti – Vedi 3.5;
- i documenti informatici prodotti dall'Utente nell'esercizio dell'attività professionale a favore della Provincia di Brescia e doverosamente inseriti nei sistemi informativi provinciali restano nella piena ed esclusiva disponibilità della Provincia di Brescia. Salvo esplicita autorizzazione scritta da parte del Dirigente responsabile, l'Utente non può formare o ottenere copia dei predetti documenti né farne alcun uso dopo la cessazione del rapporto di lavoro.
- non è assolutamente consentito il salvataggio di dati sensibili e/o giudiziari sui singoli personal computer o su altri strumenti informatici o elettronici; i dati sensibili e/o giudiziari, anche allo scopo di ottemperare agli obblighi di back-up e disaster recovery per il ripristino di tali dati previsto dalla normativa in materia, devono essere salvati unicamente nelle apposite unità di rete predisposte su indicazione del Dirigente responsabile ovvero negli applicativi gestionali di riferimento;
- tutti i files memorizzati sono da considerarsi documentazione di lavoro di proprietà e stretta disponibilità della Provincia di Brescia nel rispetto della normativa sui diritti d'autore, sui brevetti, sul segreto professionale che i dipendenti siano tenuti a rispettare.

3.14 Utilizzo di attrezzature per il lavoro in mobilità (tablet, ecc.)

Il salvataggio e backup periodico dei dati memorizzati sugli apparati (app installate, configurazioni, file, ecc.) è a carico dell'assegnatario. In caso di guasto hardware i dati potrebbero infatti non essere recuperabili.

3.14.1 Software

E' fatto divieto assoluto dell'utilizzo e/o possesso di software illegalmente copiato o comunque privo di regolare licenza d'uso.

Per quanto riguarda le app installate sugli smartphone e tablet assegnati:

- non effettuare manomissioni gravi e/o volontarie di parti interne/esterne, aperture forzate dell'apparato, alterazioni software che si manifestano come conseguenza di azioni dolose o volontarie e che rendono l'apparato non riparabile;
- conformarsi a ogni eventuale istruzione e comunicazione dell'operatore di telefonia mobile concernente la corretta utilizzazione del servizio;
- eseguire backup periodici dei dati personali memorizzati sul dispositivo;
- per ragioni di sicurezza personalizzare al primo accesso la password (modificandola con periodicità);
- non rimuovere le applicazioni di servizio autoinstallate e/o modificare le configurazioni standard impostate dall'amministratore di sistema;
- non eseguire procedure che permettano di installare applicazioni e pacchetti alternativi a quelli ufficiali previsti dall'Apple Store ovvero dal Play Store (eseguire ad esempio jailbreak sugli apparati IOS).

3.15 Utilizzo dei telefoni

Il telefono aziendale affidato all'Utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza e comunque nei limiti di quanto previsto all'art. 2.2.

Nell'utilizzo dei sistemi di telefonia, l'Utente deve osservare le seguenti regole:

- provvedere alla custodia delle attrezzature secondo quanto previsto all'art. 5.1;
- senza l'esplicito consenso dell'interlocutore remoto, è vietata la registrazione vocale delle conversazioni intercorse fra gli utenti interni tra loro e con gli utenti esterni;
- l'uso del sistema di telefonia è limitato/autorizzato all'orario di servizio o di eventuale reperibilità o attività inerenti alle mansioni svolte presso l'ente;
- è vietato l'uso dei sistemi di telefonia per le chiamate a numeri a valore aggiunto, compresa la dettatura di telegrammi, ad eccezione di quelle necessarie per ragioni di servizio e autorizzate per iscritto dal proprio Dirigente;
- è vietato effettuare operazioni di programmazione;
- è vietato collegare ai telefoni apparecchiature non espressamente autorizzate dal Settore che gestisce il "sistema informatico/informativo" dell'Ente (ad es. segreteria telefoniche o altro);
- l'apparato deve essere restituito al Settore che gestisce il "sistema informatico/informativo" dell'Ente in caso di inutilizzo.

L'uso indebito delle dotazioni telefoniche aziendali comporterà, a carico del trasgressore, la possibile apertura a suo carico di una procedura disciplinare.

L'Ente utilizza, sia a propria tutela che per un efficace controllo dei costi, un sistema di documentazione addebiti telefonici che archivia tutte le telefonate uscenti ed i costi generati dal singolo telefono aziendale. L'archivio rispetta le normative di tutela della privacy omettendo l'indicazione delle ultime tre cifre del numero chiamato.

3.15.1 Telefonia fissa

La Provincia di Brescia fornisce l'accesso al sistema di telefonia fissa a tutti gli utenti che ne abbiano necessità per motivi di servizio.

A tal fine, gli utenti hanno a disposizione unicamente gli apparati telefonici forniti dalla Provincia di Brescia. Per ragioni di sicurezza e di compatibilità con i sistemi in uso, gli utenti non sono autorizzati ad utilizzare dispositivi differenti.

La fornitura di un apparato telefonico e di uno o più interni deve essere richiesto esclusivamente dal Dirigente responsabile, così come eventuali abilitazioni aggiuntive che potrebbero implicare costi per l'Ente (vedi ad esempio l'abilitazione alle chiamate a numerazioni speciali).

L'Utente avrà la possibilità di gestire una propria rubrica utilizzando l'applicativo messo a disposizione. Il salvataggio dei dati memorizzati in tale rubrica sono a carico dell'Utente stesso che si dovrà far carico anche di spostarli in caso di variazione dell'interno assegnatogli. Le istruzioni d'uso sono disponibili sulla intranet.

3.15.2 Telefonia mobile

Il Dirigente responsabile, sulla base delle esigenze di servizio, può richiedere di dotare l'Utente di un apparato di telefonia mobile e/o di una SIM.

Qualora il Dirigente responsabile assegni un cellulare aziendale ad un Utente, quest'ultimo ne sarà responsabile sia dell'utilizzo che della custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere comunicazioni (voce, sms, mms, dati, ecc.) di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo, cioè anche per fini personali, del telefono cellulare aziendale è possibile soltanto in presenza di preventiva attivazione del servizio di "dual billing", cioè l'attivazione di un contratto con l'operatore di telefonia mobile per il riconoscimento e l'addebito del traffico personale.

All'assegnatario di dotazioni cellulari è fatto espresso divieto di:

- rimuovere la SIM dal telefono mobile aziendale per installarla su apparecchio diverso rispetto a quello assegnato - salvo casi di temporanea necessità;
- utilizzare il telefono in dotazione per usi personali o comunque per fini diversi da quelli aziendali (salvo l'abilitazione all'addebito personale);

L'assegnatario si assume ogni responsabilità derivante dall'utilizzo dell'apparato e della SIM e pertanto tutte le comunicazioni effettuate tramite l'utenza assegnatagli si presumono effettuate dall'assegnatario stesso e/o con il suo consenso. Si dovrà inoltre attenere a tutte le indicazioni previste dalla "lettera di assegnazione" che l'Utente sottoscriverà per accettazione all'atto della consegna delle attrezzature stesse.
Il salvataggio e backup periodico dei dati memorizzati sugli apparati (app installate, configurazioni, file, ecc.) e sulla SIM (rubrica) è a carico dell'assegnatario. In caso di guasto hardware i dati potrebbero infatti non essere recuperabili.

Art. 4. DISPOSIZIONI SULL'UTILIZZO DEI SERVIZI INTERNET

4.1 Navigazione web

L'accesso alle risorse web, tramite Lan, è consentito unicamente agli utenti in possesso delle credenziali di autenticazione al dominio.

La Provincia di Brescia fornisce l'accesso internet per l'utilizzo inerente alle attività lavorative a tutti gli utenti dotati delle credenziali di accesso al dominio. L'abilitazione alla navigazione web su ambienti particolari deve essere richiesta dal Dirigente responsabile.

La Provincia di Brescia mette a disposizione degli utenti i programmi necessari per navigare in internet ed utilizzare i servizi internet, elencati nell'Allegato F alle presenti "Linee guida". Gli Utenti sono tenuti ad utilizzare unicamente i web browser compresi in detto elenco, salvo che, per particolari esigenze, da comunicare tramite richiesta del Dirigente di riferimento, sia necessaria l'installazione di applicativi differenti.

Per ovvie ragioni di sicurezza non debbono essere utilizzate le opzioni di "compilazione automatica" o "ricorda password", presenti nei browser o in altre applicazioni.

4.1.1 Profili di autorizzazione

Sono previsti diversi profili di abilitazione che consentono la navigazione su determinate categorie di siti web (a seconda della classificazione del sito), in base alle esigenze lavorative di ogni Utente – Vedi allegato L.

Sulla base di quanto richiesto dal singolo Dirigente, ad ogni Utente di dominio viene associato un profilo di navigazione. I criteri di filtraggio dei siti web verranno approfonditi nell'art. 4.1.2.

4.1.2 Strumento di web content filtering

La navigazione sui siti web è regolata mediante l'adozione di opportuni applicativi di filtraggio, che si basano sulla classificazione dei siti secondo le diverse categorie di appartenenza. In relazione al profilo assegnato, vi sono categorie sulle quali un Utente può navigare e categorie sulle quali la navigazione gli è inibita. Le assegnazioni degli utenti ai differenti profili di autorizzazione vengono effettuate sulla base delle attività lavorative normalmente svolte e possono essere derogate solo in presenza di particolari esigenze, previa richiesta del Dirigente di riferimento. È comunque bloccata la navigazione su siti web potenzialmente lesivi per l'infrastruttura.

L'elenco delle categorie di filtraggio dei siti web, contenuto nell'Allegato H alle presenti "Linee guida", è soggetto ad aggiornamento periodico in considerazione della rapidità di cambiamento del web e delle tecnologie per il filtraggio dei siti.

Il firewall che presidia la rete provinciale è configurato per effettuare un filtraggio delle porte di rete, al fine di impedire l'accesso a servizi non autorizzati.

4.1.3 Regole per la navigazione web

Per la navigazione in internet l'Utente deve attenersi alle seguenti regole:

- la navigazione web è consentita unicamente nei siti i cui contenuti siano compresi nelle categorie corrispondenti al proprio profilo di navigazione - vedi art. 4.1.1;

- durante l'orario di servizio, non è consentita la navigazione web se non per esigenze attinenti allo svolgimento dell'attività lavorativa;
- non è consentito l'utilizzo di servizi web proxy o di servizi web di anonimizzazione al fine di eludere i filtri e le regole di sicurezza implementate dalla Provincia di Brescia;
- non è consentito il download, la copia, il salvataggio, l'installazione o l'utilizzo di software prelevato da siti internet, senza espressa autorizzazione del proprio Dirigente e comunque previa verifica dell'attendibilità dei siti in questione;
- non è consentito l'uso di software di condivisione di risorse (peer to peer o similari), senza espressa autorizzazione del proprio Dirigente o da persona da questi delegata;
- non è consentito l'uso di software di telefonia su IP (VOIP), di instant messaging o di videoconferenza se non espressamente autorizzati dal proprio Dirigente o da persona da questi delegata;
- è vietata ogni forma di registrazione a nome della Provincia o fornendo i dati relativi a e-mail provinciale a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat, di social network, di strumenti di condivisione, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nickname) se non espressamente autorizzati dal proprio Dirigente;
- sulle attrezzature collegate alla rete aziendale è consentita la navigazione solo ed esclusivamente tramite LAN;
- non è consentito il download, la copia o il salvataggio di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- ferme restando le attività dell'amministratore di sistema di implementazione, configurazione e gestione dei software antivirus presenti nel sistema informatico, spetta all'Utente sottoporre a verifica tutti i file di provenienza incerta ancorché attinenti all'attività lavorativa, tramite gli strumenti antivirus in dotazione. Le istruzioni operative sull'utilizzo del software antivirus sono contenute nell'Allegato J alle presenti "Linee guida".

4.2 Posta elettronica aziendale

Le caselle di posta fornite dalla Provincia di Brescia devono essere dedicate alle comunicazioni ufficiali sia interne che esterne.
Il sistema di posta elettronica è Microsoft Outlook 365. Il contenuto della singola casella (rubrica, agenda, messaggi di posta, ecc.) è memorizzata su un server esterno all'Ente e viene salvato quotidianamente
L'accesso avviene in modalità differente, a seconda del tipo di casella utilizzato. Tutte le indicazioni di dettaglio sono disponibili sulla intranet.

Tutte le caselle prevedono una dimensione massima che varia in base all'ambiente utilizzato, fatte salve le eventuali specifiche abilitazioni richieste dal Dirigente responsabile. Tali dimensioni vengono definite nell'0.

L'accesso al servizio di posta elettronica da parte di un Utente avviene mediante delle credenziali di autenticazione (nome Utente e password). Per le caselle nominative l'accesso avviene mediante le credenziali di accesso al dominio.

Gli utenti assegnatari delle caselle di posta elettronica sono i diretti responsabili del corretto utilizzo delle stesse e rispondono personalmente dei contenuti trasmessi.

Le e-mail relative ad ogni account restano nella piena ed esclusiva disponibilità della Provincia di Brescia.

Su richiesta del Dirigente responsabile, il Settore che gestisce il "sistema informatico/informativo" dell'Ente, può rilasciare ai singoli settori caselle di posta certificata (PEC). Tali caselle potranno essere integrate al programma di Protocollo.

4.2.1 Account di posta elettronica nominativa

Previa richiesta del proprio Dirigente, viene fornito un account nominativo di Posta Elettronica, con dominio istituzionale. Gli account di posta elettronica istituzionali avranno, di norma, il seguente formato: *inizialenomecognome@provincia.brescia.it* e *inizialenomecognome@provincia.bs.it* (ad esempio mrossi@provincia.brescia.it - mrossi@provincia.bs.it). I casi di omonimia sono gestiti distintamente.

La casella di posta elettronica aziendale assegnata all'Utente è uno strumento di lavoro il cui utilizzo per fini personali non è consentito se non nei limiti di cui all'art. 2.2. Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e sono responsabili del contenuto delle proprie comunicazioni e della riservatezza dei dati ivi contenuti, la cui impropria colpevole diffusione potrebbe integrare l'illecito di violazione del segreto d'ufficio o della normativa in materia di tutela dei dati personali

La casella di posta elettronica non è da intendersi come corrispondenza privata del singolo dipendente ma esclusivamente quale corrispondenza e documentazione di lavoro di stretta pertinenza aziendale. Qualora l'Amministratore di Sistema, nell'espletamento delle proprie funzioni, individui comportamenti anomali potenzialmente pericolosi per i sistemi informativi aziendali, potrà inviare un avviso generalizzato o circoscritto agli utenti afferenti il settore in cui stato rilevato il comportamento anomalo con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite; contrariamente il datore di lavoro potrà effettuare controlli sulla singola casella di posta elettronica, anche tramite propri incaricati, con identificazione del mittente, del destinatario e dell'oggetto di ogni mail.

Le caselle di posta individuali hanno validità pari alla durata della permanenza in servizio dell'Utente. Nel caso in cui l'Utente non presti più la sua attività lavorativa presso la Provincia di Brescia, la casella di posta elettronica sarà prontamente disattivata. Su richiesta del Dirigente responsabile, con un preavviso di almeno 5 giorni lavorativi rispetto alla data di cessazione, la casella di posta potrà restare attiva per un massimo di ulteriori 3 mesi dalla data di cessazione del rapporto di lavoro, durante il quale sarà inserita una risposta automatica d'ufficio.

4.2.2 Account di posta elettronica non nominativi, alias e liste di distribuzione (mailing list)

In caso di particolari esigenze di servizio, allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è possibile creare account di posta elettronica non nominativi (ad esempio account di settore, di progetto o di una particolare attività o funzione condivisa):

- sportellocaccia@provincia.brescia.it
- segreteria.informatica@provincia.brescia.it
- cpi_brescia@provincia.brescia.it

La richiesta di attivazione di una lista di distribuzione deve essere avanzata da parte del Dirigente responsabile e deve contenere l'elenco dei nominativi che devono essere inseriti nella relativa lista di distribuzione. Questi account di posta possono essere gestiti da uno o più utenti e possono essere creati in modo tale che la posta venga salvata sul server (casella non nominativa) oppure che venga automaticamente reindirizzata alle singole caselle nominative degli utenti delegati (liste di distribuzione).

Il Dirigente responsabile è tenuto a verificare, almeno annualmente, la necessità di mantenere attive le liste di distribuzione a lui afferenti e l'elenco dei nominativi abilitati.

Questi indirizzi di posta potranno essere utilizzati nelle pubblicazioni cartacee, a carattere informativo realizzate dalla Provincia e/o pubblicate sul portale Internet della Provincia di Brescia.

Occorre incentivare e favorire l'uso di tali liste evitando trasmissioni al singolo dipendente ma favorendo gli invii delle comunicazioni formali da indirizzi di struttura verso le liste delle strutture cui afferiscono i destinatari. Per facilitare lo scambio di informazioni funzionali alle attività svolte, è possibile far attivare più liste all'interno dello stesso settore che rispecchino particolari funzioni: la soluzione deve essere funzionale all'organizzazione del settore e degli uffici e all'ottimizzazione della comunicazione interna e per questo, quindi, deve rispondere a principi di semplificazione.

Al fine di non duplicare le comunicazioni è opportuno che una comunicazione e-mail inviata ad una lista di distribuzione non venga anche contemporaneamente inviata all'indirizzo individuale.

4.2.3 Client di posta elettronica

Il Settore che gestisce il "sistema informatico/informativo" dell'Ente mette a disposizione degli utenti alcuni applicativi per l'utilizzo della casella di posta elettronica istituzionale, elencati nell'0 alle presenti "Linee guida". Gli utenti sono autorizzati ad utilizzare solamente i client di posta elettronica presenti in elenco.

4.2.4 Accesso alla casella nominativa di un Utente assente - Designazione fiduciario

Nel ricordare che le comunicazioni d'ufficio dovrebbero transitare dal sistema di protocollo, potrebbe rendersi necessario utilizzare la propria casella di posta per comunicazioni d'ufficio.

In caso di assenza improvvisa o prolungata e in presenza di improrogabili necessità di servizio, potrebbe essere necessario accedere al contenuto della casella di posta elettronica aziendale di un utente.

Il Dirigente responsabile invia al Direttore del Settore che gestisce il "sistema informatico/informativo", in forma scritta, motivata richiesta di accesso alla casella.

Il Direttore del Settore che gestisce il "sistema informatico/informativo" autorizza gli amministratori di sistema a delegare il Dirigente richiedente sulla casella. La delega consentirà al Dirigente di accedere al contenuto della casella di posta e a tutti i servizi Office 365 (ad esempio calendario, onedrive, ecc.). Al termine del recupero dei dati il Dirigente responsabile darà comunicazione, sempre in forma scritta, che la delega può essere rimossa.

Il Dirigente responsabile, se lo ritiene opportuno, potrà comunicare la procedura effettuata all'utente interessato.

4.2.5 Risposta automatica ai messaggi ricevuti (o messaggio di fuori sede) - Assenza programmata o imprevista

In caso di assenza programmata ogni Utente è tenuto ad attivare la procedura di risposta automatica ai messaggi ricevuti. Procedura messa a disposizione dai software per la consultazione della posta elettronica; il messaggio di risposta automatica deve contenere indicazioni relative ad un altro soggetto a cui fare riferimento o altre modalità di contatto dell'Ente e il periodo di assenza. Le istruzioni operative sull'uso del messaggio di assenza dall'ufficio sono contenute nell'Allegato I alle presenti "Linee guida".

In caso di eventuali assenze non programmate (ad es. per improvvisa malattia), qualora l'Utente non possa attivare la procedura sopra descritta, il Dirigente di riferimento ha facoltà di richiedere, in forma scritta al Direttore del Settore che gestisce il "sistema informatico/informativo" l'attivazione della procedura di risposta automatica. Gli amministratori di sistema provvederanno ad impostare il messaggio di risposta

automatica. È compito del Dirigente responsabile informare dell'accaduto l'Utente interessato mediante comunicazione scritta.

4.2.6 Note in calce ai messaggi inviati

Ogni Utente può definire di aggiungere in calce ai messaggi di posta elettronica una propria firma – Vedi Allegato K.

4.2.7 Filtro sulle e-mail

Al fine di garantire un elevato livello di sicurezza del sistema informativo, l'infrastruttura di rete della Provincia di Brescia è dotata di uno strumento di filtraggio automatico della posta elettronica, che svolge attività di antispam e antiphishing. Inoltre vengono filtrate alcune tipologie di allegati, in relazione all'estensione dei file e alla loro dimensione (vedi art. 4.2.8).

4.2.8 Regole per la posta elettronica

Per l'utilizzo della posta elettronica, fermo restando l'obbligo di rispetto del segreto postale, l'Utente deve attenersi alle seguenti regole:

- è vietato l'invio di messaggi di posta elettronica interna ad un numero indistinto di utenti (tutti gli utenti o liste di distribuzione), salvo i casi di comprovata necessità organizzativa che andranno appositamente e preventivamente autorizzati dal Settore che gestisce il "sistema informatico/informativo" dell'Ente (per non caricare troppo il traffico di rete è buona norma pianificarne l'invio al di fuori degli orari di servizio);
- non utilizzare il servizio per scopi illegali o non conformi alle presenti "Linee guida" o in maniera tale da recar danno o pregiudizio alla Provincia di Brescia o a terzi;
- non utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con la fruibilità del servizio da parte degli altri utenti;
- non inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non 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 ad esempio a:
    - pubblicità non istituzionale, manifesta o occulta;
    - prodotti di natura politica;
    - comunicazioni commerciali private;
    - materiale pornografico o simile;
    - materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
    - materiale che violi la legge sulla privacy;
    - contenuti o materiali che violino i diritti di proprietà di terzi;
    - altri contenuti illegali.
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list se non per motivi inerenti l'attività lavorativa svolta;
- non sono consentita la trasmissione e la ricezione di testi o documenti contenenti dati sensibili e/o giudiziari. I documenti o i testi recanti dati sensibili e/o giudiziari che pervenissero comunque sulle caselle di posta istituzionali, via posta elettronica non certificata, devono essere immediatamente cancellati;
- è vietato scaricare come allegati files eseguibili (ad esempio aventi estensione .exe .bat .com .pif .scr);

- ferme restando le attività dell'amministratore di sistema di implementazione, configurazione e gestione dei software antivirus presenti nel sistema informatico, spetta all'Utente sottoporre a verifica tutti i file di provenienza incerta ancorché attinenti all'attività lavorativa, tramite gli strumenti antivirus in dotazione. Le istruzioni operative sull'utilizzo del software antivirus sono contenute nell'0 alle presenti "Linee guida". Particolare attenzione andrà posta ai files compressi (ad esempio aventi estensione .zip .gz .tar) e ai files aventi doppia estensione (ad esempio .txt, .exe, .jpg. oppure .exe) indipendentemente dal fatto che provengano o sembrino provenire da un mittente noto;
- non è consentito l'utilizzo dell'account di posta elettronica istituzionale per effettuare attività definibili come spam;
- in nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili;
- non è consentito l'invio di messaggi di natura ripetitiva (catene di S. Antonio) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Di seguito si elencano alcune norme di comportamento che ciascun Utente è tenuto ad osservare al fine di preservare l'efficienza del servizio di posta elettronica e delle comunicazioni con esso veicolate:

- l'Utente è tenuto a visionare regolarmente la casella di posta elettronica di propria competenza;
- i messaggi devono essere preferibilmente di solo testo, evitando ove possibile ogni formattazione e inserzione di immagini;
- è buona norma inviare messaggi sintetici che descrivano in modo chiaro il contenuto;
- è necessario indicare sempre chiaramente l'oggetto, in modo tale che il destinatario possa immediatamente individuare l'argomento del messaggio ricevuto, facilitandone la successiva ricerca per parola chiave;
- consigliabile non superare la dimensione complessiva di 5 MB degli allegati inviati con un singolo messaggio. Nel caso in cui il messaggio sia inviato a più destinatari la dimensione dell'allegato va moltiplicata per il numero dei destinatari e non può superare il limite sopra indicato;
- per inviare allegati di dimensioni superiori di cui al punto precedente è possibile utilizzare l'apposito servizio messo a disposizione al link http://edes.provincia.brescia.it , con il quale è possibile trasferire files di dimensioni fino a 200Mb. Questi file resteranno disponibili per un tempo limitato (max 45 giorni solari). L'accesso al servizio avviene tramite le credenziali di dominio. Per l'invio di file di dimensioni ancora superiori contattare i tecnici del Settore che gestisce il "sistema informatico/informativo" dell'Ente;
- limitare l'invio di messaggi di posta elettronica a indirizzi plurimi (decine di destinatari) e trasmetterli solo in casi motivati da esigenze di servizio;
- le caselle di posta hanno una dimensione predefinita e non estendibile, occorre pertanto mantenere in ordine la propria casella di posta provvedendo a ripulirla con regolarità (ad esempio salvando gli allegati ingombranti, eliminando le mail non ritenute utili, ecc.). Oltre tali limiti infatti la casella potrebbe non funzionare correttamente.

4.3 Log dei servizi di rete

L'infrastruttura di rete della Provincia di Brescia basa il proprio funzionamento su una serie di servizi di rete, i quali consentono di instaurare una comunicazione dati tra due o più dispositivi (pc, server, stampanti, ecc.) e generano una registrazione di tutte le operazioni compiute. Tali registrazioni, dette "log", per motivi di sicurezza e di diagnostica vengono conservate per un determinato periodo di tempo sotto forma di "log files".

I “log files” generati dai singoli servizi o dai singoli sistemi di base (DHCP, DNS, NAT, ecc.) non consentono di associare un Utente all'attività da questi svolta; in altri termini, a titolo di esempio, non permettono di tracciarne la navigazione web o gli accessi alle risorse.

L'ordinaria attività di analisi dei log dei singoli sistemi, che viene svolta dagli amministratori di sistema per motivi di diagnostica, non costituisce pertanto trattamento di dati personali.

Tuttavia, a seguito del verificarsi di incidenti informatici, anomalie o malfunzionamenti dell'infrastruttura di rete, gli amministratori di sistema potrebbero avere la necessità di mettere in correlazione i log dei singoli sistemi per individuare la causa o l'origine del problema. Le elaborazioni derivanti dall'associazione dei log provenienti da due o più servizi di rete, potrebbero contenere dati personali anche sensibili. In tale evenienza, la sola finalità legittimante il trattamento è circoscritta alla gestione dell'incidente informatico oggetto di analisi.

Al di fuori dei casi sopra descritti, la Provincia di Brescia non consente che sia effettuata alcuna attività di analisi e aggregazione dei log per finalità di controllo diretto o indiretto dell'operato degli utenti.

4.3.1 Log dei servizi di sicurezza

Nell'infrastruttura della Provincia di Brescia sono presenti servizi di rete avanzati, la cui adozione è obbligatoria o consigliata dalle citate norme a tutela della privacy per ragioni di sicurezza, protezione dati e prevenzione. Alcuni di questi servizi, tra cui Firewall, Proxy Server, Web Filtering (descritti nelle presenti “Linee guida”) possono indirettamente raccogliere e conservare dati personali o sensibili riferibili agli utenti o a terze persone, identificate o identificabili. Le operazioni che la Provincia di Brescia svolge su tali dati, nonché le modalità di utilizzo dei medesimi, sono precisate nei paragrafi seguenti.

4.3.2 Log della navigazione Internet

L'applicativo di web filtering (vedi art. 4.1.2) genera un log per ogni richiesta di consultazione di una pagina web, contenente le seguenti informazioni: *url richiesta, indirizzo IP e username dell’Utente*. Il log generato è necessariamente nominativo in ragione del fatto che il permesso o il diniego alla consultazione vengono decisi sulla base del profilo di navigazione al quale appartiene l’Utente richiedente. L’intero processo di generazione e salvataggio dei log è svolto in forma automatica e quotidiana.

Le modalità di generazione e raccolta dei log è necessaria per ragioni di produttività e di sicurezza dei sistemi e dei dati, oltre che per consentire eventuali controlli in caso di incidenti.

Automaticamente vengono anche generati report aggregati relativi alla navigazione web, suddivisi per Settore, che potrebbero essere inviati anche con periodicità mensile ai rispettivi Dirigenti, per consentire la verifica del rispetto delle disposizioni delle presenti “Linee guida”, onde eventualmente attivare le procedure previste dall’art. 6.3 delle presenti “Linee guida” in presenza di eventuali comportamenti anomali.

4.3.3 Periodo Conservazione dei log della navigazione Internet

I log di navigazione relativi al **diniego di accesso** ad una pagina web vengono conservati in file giornalieri per 90 giorni, al solo scopo di poter analizzare eventuali anomalie o correggere impostazioni di filtraggio eccessivamente restrittive, anche su segnalazione degli utenti.

I log di navigazione relativi al **consenso di accesso** ad una pagina web vengono salvati in file giornalieri e conservati per un massimo di 90 giorni.

La Provincia di Brescia dispone la conservazione di questi log unicamente per ragioni di sicurezza e non ne è consentito l'utilizzo a titolo di controllo diretto e preventivo degli utenti.

Al verificarsi di un incidente informatico, riconducibile alla navigazione web, anche su richiesta di un Dirigente, i log della navigazione vengono analizzati dagli amministratori di sistema, al fine di circoscrivere l'area di indagine e individuare l'origine dell'incidente.

4.3.4 Cronologia delle pagine web visitate

La cronologia, la memoria cache (files temporanei) e i cookies relativi alle pagine web visitate sono memorizzati nel profilo dei singoli utenti e conservati in locale sul computer utilizzato, ad eccezione di quanto accade per la navigazione effettuata tramite i servizi Citrix, nel qual caso vengono conservati sul file server di Citrix. In entrambi i casi è possibile la cancellazione, a carico del singolo utente, come da procedura contenuta nell'Allegato F alle presenti "Linee guida"; per quanto riguarda la pulizia di tali file sui server Citrix è però necessario che venga effettuata prima di chiudere la sessione di lavoro.

È consigliabile cancellare periodicamente dalla propria postazione di lavoro le informazioni sopra indicate. Questo consente di liberare lo spazio occupato su disco oltre che proteggere la riservatezza della propria navigazione.

4.3.5 Log dei servizi di posta elettronica

I log di transito della posta elettronica provinciale e dei relativi sistemi di filtraggio vengono conservati al massimo per un periodo di 90 giorni.

4.4 Statistiche

Ai soli fini statistici, con periodicità predefinita (giorno, mese, anno, ecc.) vengono generati report in forma anonima e aggregata relativamente all'intero Ente sulla base di alcuni parametri di navigazione e utilizzo dei sistemi informatici. Ad esempio, è possibile ottenere report relativi a:

- siti visitati
- file scaricati
- n° connessioni
- byte scaricati
- tempo e orari di navigazione
- protocolli utilizzati
- browser utilizzati

Art. 5. ULTERIORI NORME COMPORTAMENTALI

5.1 Custodia dotazione assegnata

Gli assegnatari delle attrezzature della Provincia di Brescia sono tenuti a garantirne il corretto utilizzo e custodia, in particolare evitando qualsiasi danneggiamento hardware e software. I beni ed i servizi informatici assegnati all'Utente sono da ritenersi a tutti gli effetti un bene di proprietà dell'Ente. Per questo motivo il loro utilizzo è consentito solo se correlato alle attività lavorative e in conformità con gli scopi dell'Ente stesso.

Ad integrazione di quanto riportato nei precedenti articoli delle presenti "Linee guida" si riportano alcune norme generali relativamente alla custodia delle attrezzature:

- non è autorizzato il collegamento alla rete aziendale LAN di attrezzature personali (ad esempio notebook personali);
- non è autorizzato il collegamento di periferiche personali alla dotazione assegnata (ad esempio chiavetta per la navigazione);
- in caso di furto o smarrimento, è obbligatorio che l'Utente sporga denuncia formale alle Autorità competenti e comunichi immediatamente il fatto al proprio Dirigente, che a sua volta ne renderà edotto il Settore Innovazione, oltre che l'Ufficio Provveditorato;
- in caso di furto e/o smarrimento di attrezzature cellulari la copia della denuncia va inviata immediatamente al Settore che gestisce il "sistema informatico/informativo" dell'Ente, azione per consentire il blocco della SIM e dell'apparato al fine di evitare utilizzi non autorizzati;
- è vietato manomettere i componenti dell'apparecchio;
- è vietato alterare l'apparecchio con pennarelli indelebili o altro (invalidandone la garanzia);
- l'assegnatario deve avere cura delle attrezzature assegnate, segnalando ogni anomalia di funzionamento al Settore che gestisce il "sistema informatico/informativo" dell'Ente;
- l'Utente è tenuto a controllare che non si verifichino accessi non autorizzati sui dispositivi in sua dotazione;
- l'Utente è tenuto a bloccare l'accesso ai propri dispositivi qualora dovesse lasciarli incustoditi anche per un breve lasso di tempo.

Ogni situazione anomala va segnalata al proprio Dirigente.

5.2 Telelavoro

Per gli utenti che usufruiscono del telelavoro restano valide tutte le norme delle presenti "Linee guida", sia che utilizzino da remoto apparati informatici personali sia messi a disposizione dalla Provincia di Brescia.

Nel caso si utilizzino attrezzature personali il Settore che gestisce il "sistema informatico/informativo" dell'Ente, non potrà erogare alcun tipo di assistenza hardware e non potrà effettuare alcuna installazione software, ad eccezione dell'antivirus. L'unica attività di assistenza riguarderà gli accessi alla rete aziendale.

Vista la presenza di informazioni riservate, di pratiche coperte da segreto d'ufficio o eventualmente di dati di servizio, l'utilizzo delle apparecchiature deve garantire un accesso riservato alle informazioni contenute e, in particolare per le attrezzature fornite dalla Provincia, l'utilizzo deve essere strettamente personale pertanto è vietata la creazione di nuovi profili Utente, ed inoltre è fatto obbligo di mantenere attivo il software antivirus installato dal Settore che gestisce il "sistema informatico/informativo" dell'Ente.

5.3 Attrezzature non fornite dal Settore Innovazione

Fermo restando quanto previsto dalle presenti "Linee guida", le attrezzature informatiche vengono fornite dal Settore che gestisce il "sistema informatico/informativo" dell'Ente o comunque a seguito della sua autorizzazione. I tecnici del Settore che gestisce il "sistema informatico/informativo" dell'Ente non erogheranno alcun tipo di assistenza e manutenzione sulle attrezzature acquisite in modalità differenti.

E' vietato connettere alla rete LAN provinciale computer o altri dispositivi personali senza l'autorizzazione del Settore che gestisce il "sistema informatico/informativo" dell'Ente. Tale autorizzazione deve essere richiesta in forma scritta dal Dirigente responsabile. In ogni caso, i dispositivi personali autorizzati dovranno assicurare il rispetto delle misure minime di sicurezza, ovvero la presenza di un software antivirus attivo ed aggiornato.

Nei casi specifici in cui il Settore voglia utilizzare attrezzature ricevute in comodato d'uso (ad esempio fornite nell'ambito di specifici progetti) è necessario:

- Che il dirigente responsabile informi preventivamente il Settore che gestisce il "sistema informatico/informativo" dell'Ente, specificando i dettagli tecnici delle attrezzature e i dati relativi all'eventuale assistenza fornita e ai termini del comodato;
- Il Settore che gestisce il "sistema informatico/informativo" dell'Ente provvederà ad effettuare le verifiche tecniche di compatibilità;
- Solo se le verifiche danno esito positivo il Dirigente Responsabile potrà richiedere la configurazione delle attrezzature nella rete aziendale.
- Il Dirigente Responsabile, al termine del comodato, deve aprire apposita richiesta per la disinstallazione di eventuali software di proprietà della Provincia ed eliminazione di eventuali dati memorizzati sul disco.

5.4 Backup e Disaster Recovery (DR)

I documenti (e dati) prodotti durante il servizio vanno salvati sulle **cartelle di rete** rese disponibili sui server dipartimentali. La definizione delle cartelle e dei relativi accessi viene richiesta dal Dirigente del settore interessato.

Ogni Utente ha inoltre a disposizione una cartella di rete "personale-nominativa" identificata con il **disco U**. In questa cartella possono essere salvati i file "personali" di lavoro che non devono essere condivisi con i colleghi. Ha una dimensione massima di 200 MegaByte. Per queste cartelle viene effettuato un backup (salvataggio) quotidiano.

Le cartelle di rete, incluse quelle personali, vengono sottoposte a backup con i seguenti criteri:

- Frequenza di backup (salvataggio): quotidiana
- Ripristino: in caso di cancellazione o modifica accidentale di un file, l'Utente può richiedere il ripristino del file. In tal caso viene effettuato il ripristino alla versione presente al momento dell'ultimo backup eseguito con successo. In base alle risorse disponibili sul sistema, potrebbe essere possibile ripristinare anche versioni meno recenti del file (tale possibilità non è garantita in tutte le situazioni). Dopo 12 mesi, eventuali file eliminati o modificati accidentalmente, diventano in ogni caso non recuperabili.

PC, notebook e dispositivi mobili non sono sottoposti a backup, pertanto eventuali file eliminati o modificati accidentalmente non possono essere recuperati.

Le cassette di **posta elettronica** Office365 sono ospitate e protette sul cloud Microsoft. I messaggi eliminati dall'Utente vengono spostati nella cartella "Posta Eliminata" dalla quale possono essere ripristinati in autonomia dall'Utente stesso. Una volta svuotata la cartella "Posta Eliminata" i messaggi restano recuperabili per un periodo aggiuntivo di 30 giorni, trascorso il quale non sono più recuperabili, né dagli amministratori di sistema della Provincia, né dal fornitore di servizi cloud.

I dati presenti negli **applicativi** vengono salvati quotidianamente. Sul PC (e sulle cartelle di rete) non vanno salvati i dati che sono comunque disponibili nei vari applicativi gestionali, in quanto si creerebbe una duplicazione delle informazioni con evidente consumo di risorse-spazio.

5.5 Attività dell'amministratore di sistema

Per i soli fini di amministrazione, gestione e manutenzione del sistema informatico, l'amministratore di sistema ha la possibilità di utilizzare oppure di connettersi da remoto alle risorse disponibili su ciascun personal computer in dotazione agli utenti e più in generale a ciascun dispositivo connesso alla infrastruttura informatica.

L'amministratore di sistema provvede ad implementare, configurare e gestire uno o più software antivirus in grado di proteggere l'infrastruttura informatica da virus e più in generale da malware (un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito). Tali software antivirus, in base alle configurazioni effettuate dall'amministratore di sistema, sono in grado automaticamente di rilevare le infezioni da virus informatici e di riparare, mettere in quarantena o eventualmente eliminare i file infetti.

Per i soli fini di amministrazione, gestione e manutenzione del sistema informatico, l'amministratore di sistema ha la possibilità di accedere a tutti i dati presenti nel sistema informatico stesso compresi i file conservati nei dischi di rete, nei dischi dei personal computer e negli altri dispositivi connessi.

L'amministratore di sistema ha inoltre la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente documento, dandone contestuale comunicazione all'Utente interessato, ove ciò sia possibile, e al Dirigente di riferimento.

All'amministratore di sistema è consentito l'uso di supporti rimovibili per le operazioni di backup dei dati. Le modalità di realizzazione, utilizzo, conservazione e distruzione dei dati di backup sono specificate nelle lettere di incarico per gli amministratori di sistema.

5.6 Assistenza applicativa e accesso ai fornitori

Nel caso in cui un settore affidi direttamente un incarico di assistenza e manutenzione applicativa che implichi il collegamento ai server e/o alle postazioni Utente è necessario che:

- Il contratto preveda la designazione all'incarico trattamento dati e/o ad amminstratore di sistema;
- Il Settore che gestisce il "sistema informatico/informativo" dell'Ente venga informato dei termini contrattuali previsti;
- Se il fornitore deve avere accesso alle risorse di rete il Dirigente responsabile deve richiedere al Settore Innovazione il rilascio delle credenziali di accesso, specificando le abilitazioni che dovranno essere concesse;

- Il Settore che gestisce il “sistema informatico/informativo” dell’Ente comunicherà al Dirigente le credenziali rilasciate, il Dirigente a sua volta dovrà formalizzare il rilascio di tali credenziali comunicandole al fornitore;
- Il dirigente responsabile, al termine del contratto, deve richiedere al Settore che gestisce il “sistema informatico/informativo” dell’Ente, la disabilitazione delle credenziali al fine di impedire accessi non autorizzati.

Si ricorda che in assenza di credenziali il fornitore potrebbe non essere in grado di adempiere agli obblighi contrattuali pertanto gli accessi andranno richiesti prima dell’avvio del servizio.

Si ricorda che è vietato connettere alla rete LAN provinciale computer o altri dispositivi personali senza l’autorizzazione del Settore che gestisce il “sistema informatico/informativo” dell’Ente. Pertanto nel caso in cui un fornitore si debba connettere all’infrastruttura di rete della Provincia di Brescia utilizzando dispositivi propri (anche solo per una demo applicativa), il Dirigente responsabile, che ha affidato l’incarico, avverte tramite posta elettronica il Settore che gestisce il “sistema informatico/informativo” dell’Ente a mezzo e-mail all’indirizzo assistenza.sistemistica@provincia.brescia.it . Un tecnico informatico verificherà che l’apparecchiatura utilizzata possieda i requisiti minimi di sicurezza e cioè che sia protetta da sistema antivirus attivo ed aggiornato. A seguito dell’esito positivo di tale verifica sarà possibile collegare il dispositivo alla rete aziendale.

5.7 Accesso ai dati personali in caso di assenza dell’Utente

In caso di assenza improvvisa o prolungata e in presenza di improrogabili necessità di servizio, potrebbe essere necessario accedere al contenuto della postazione utente di un Utente.

Premesso che tutti i file di servizio devono essere salvati nelle directory di rete, se dovesse rendersi necessario accedere ai file memorizzati in locale su una postazione utente il Dirigente responsabile deve inviare al Direttore del Settore che gestisce il “sistema informatico/informativo”, in forma scritta, motivata richiesta di accesso ai dati.

Il Direttore del Settore che gestisce il “sistema informatico/informativo” autorizza gli amministratori di sistema ad accedere ai dati e a recuperare i files necessari, spostandoli nelle apposite cartelle di rete.

5.8 Movimentazione attrezzature

La movimentazione delle attrezzature tra uffici e/o tra settori deve essere autorizzata dal Dirigente responsabile che informa preventivamente il Settore che gestisce il “sistema informatico/informativo” dell’Ente e l’Ufficio Provveditorato, al fine di mantenere aggiornato l’inventario dei beni mobili dell’Ente.

Il Settore che gestisce il “sistema informatico/informativo” dell’Ente pianifica l’adeguamento tecnologico del parco esistente. In nessun caso sono ammesse movimentazioni di postazioni tra Utenti.

La movimentazione può riguardare casistiche differenti:

- L’attrezzatura è inutilizzata pertanto deve essere resa al Settore che gestisce il “sistema informatico/informativo” dell’Ente. Questo consente l’ottimizzazione delle risorse a disposizione dell’Ente. Il Settore che gestisce il “sistema informatico/informativo” dell’Ente infatti ha un magazzino nel quale custodisce le attrezzature non utilizzate e le rende disponibili per eventuali nuove assegnazioni

- L'Utente viene trasferito ad altro ufficio all'interno del medesimo settore: il Dirigente responsabile deve richiedere la cessazione delle abilitazioni non più utilizzate e contestualmente richiedere le nuove abilitazioni che devono essere rilasciate
- L'Utente viene trasferito ad altro settore: vedi art. 5.10
- L'Utente cessa il servizio – vedi art. 5.9
- Il Dirigente responsabile richiede la sostituzione della postazione con una di nuova fornitura e/o con una presente a magazzino: all'Utente viene fornita la nuova attrezzatura e contestualmente viene ritirata quella in uso.

5.9 Cessazione del rapporto lavorativo

In caso di cessazione del rapporto lavorativo (licenziamento, pensionamento, trasferimento presso altro ente, temine del contratto, ecc.) l'Utente dovrà:

- restituire eventuali attrezzature a lui assegnate;
- rendere disponibili sulle cartelle di rete eventuali files inerenti l'attività lavorativa (rendendoli disponibili ai colleghi che lo sostituiranno);
- eliminare eventuali dati personali presenti sui dispositivi in dotazione (PC, telefono, cellulare, ecc.).

Il Dirigente responsabile dovrà informarne il Settore che gestisce il "sistema informatico/informativo" dell'Ente, almeno tre giorni lavorativi prima della data di cessazione, e dovrà:

- comunicare al Settore che gestisce il "sistema informatico/informativo" dell'Ente la cessazione dell'Utente e la data di conclusione delle attività lavorative presso il Settore;
- richiedere la disabilitazione degli accessi agli applicativi gestionali (atti, protocollo, contabilità, fax server, ecc.) e ad eventuali liste di distribuzione;
- accertarsi che eventuali liste di distribuzione e le numerazioni di faxserver attive sia ricevute da altri utenti ed eventualmente richiedere l'abilitazione di accesso a nuovo Utente;
- comunicare il nuovo assegnatario sia della postazione di lavoro che dell'interno e dell'apparato telefonico. Nel caso in cui le attrezzature non venissero riassegnate dovranno essere restituite al Settore che gestisce il "sistema informatico/informativo" dell'Ente che le renderà disponibili per altri settori;
- farsi restituire eventuali dotazioni mobili (cellulari, tablet, notebook, ecc.) e consegnarle al Settore che gestisce il "sistema informatico/informativo" dell'Ente. Su richiesta dell'Utente, il Dirigente potrà eventualmente autorizzare la voltura della SIM (in tal caso la comunicazione dovrà essere inviata al Settore che gestisce il "sistema informatico/informativo" dell'Ente che provvederà ad inoltrare all'operatore di telefonia mobile la richiesta di voltura "a privato");
- comunicare le motivazioni diverse rispetto ai cinque punti precedenti motivandole ed dettagliandole.

A seguito della comunicazione i tecnici informatici provvederanno ad inibire gli accessi al dominio, alla navigazione internet, all'accesso alle cartelle di rete e agli applicativi, oltre che ad eliminare la casella di posta elettronica nominativa e il contenuto del disco U dell'Utente. La postazione di lavoro e l'apparato telefonico verranno riconfigurati per il nuovo assegnatario e gli eventuali dati presenti (relativi a precedenti assegnatari) verranno definitivamente eliminati ovvero verranno ritirati, resettati e resi disponibili per la riassegnazione.

Nel caso in cui il Settore che gestisce il “sistema informatico/informativo” dell’Ente, venisse informato sulla data di cessazione direttamente dal Settore Personale, o da eventuali automatismi generati dall’integrazione delle basi dati esistenti, le credenziali verranno automaticamente disattivate. In particolare verranno cessati l'accesso al dominio e alla navigazione internet, mentre la casella di posta elettronica sarà eliminata dal server, così come il contenuto della cartella di rete "disco U". Resta poi a carico del Dirigente responsabile comunicare le altre informazioni sopra descritte.

5.10 Trasferimento Utente tra settori

In caso di trasferimento presso altro settore deve essere inviata informativa al Settore che gestisce il “sistema informatico/informativo” dell’Ente.

In particolare il Dirigente del settore di origine, secondo quanto dettagliatamente indicato all’5.9 del presente documento, deve:

- comunicare al Settore Settore che gestisce il “sistema informatico/informativo” dell’Ente, il trasferimento dell’Utente e la data di conclusione delle attività lavorative presso il settore;
- richiedere la disabilitazione di accesso ai sistemi informativi (applicativi, faxserver, navigazione internet, ecc.), alle cartelle di rete e alle liste di distribuzione;
- comunicare l'eventuale riassegnazione del PC, dell'interno e dell’apparato telefonico a nuovo Utente ovvero autorizzare il trasferimento delle attrezzature presso il nuovo settore. In quest’ultimo caso deve comunicare anche all'Ufficio Provveditorato lo scarico dall'inventario del bene e la nuova assegnazione;
- comunicare al Dirigente del settore di destinazione l’eventuale dotazione di materiale cellulare e mobile (ad es. notebook, tablet, ecc.).

Il Dirigente del settore di destinazione può:

- richiedere l’eventuale abilitazione di accesso ai sistemi informativi, alle cartelle di rete e alle liste di distribuzione;
- autorizzare per iscritto il mantenimento dell’assegnazione delle attrezzature cellulari e mobili ovvero richiederne la restituzione, dandone comunicazione anche al Settore Settore che gestisce il “sistema informatico/informativo” dell’Ente.

L’Utente:

- con almeno tre giorni lavorativi di anticipo, rispetto alla data di trasferimento, deve comunicare al Settore che gestisce il “sistema informatico/informativo” dell’Ente se il contenuto della casella di posta elettronica nominativa dovrà essere trasferito sulla postazione in uso presso il settore di destinazione;
- nel caso in cui la postazione utilizzata sia stata trasferita dal settore di origine deve informare il Settore che gestisce il “sistema informatico/informativo” dell’Ente dello spostamento. I tecnici interverranno per riconfigurare la postazione. In particolare sul PC verranno eliminate le precedenti stampanti e condivisioni di rete e verranno installate le nuove, verranno disinstallati i software licenziati per il settore di origine e verrà eliminato il profilo Utente. Per quanto riguarda invece l’apparato telefonico verrà riconfigurato per il nuovo settore e verranno eliminate tutte le abilitazioni specifiche relative al settore di origine;
- nel caso in cui utilizzi una nuova postazione (messa a disposizione dal settore di destinazione) deve richiederne la configurazione (ad es. stampanti di rete).

5.11 Assenze per lunghi periodi (aspettative, maternita', ecc.)

In caso di assenze per lunghi periodi l'Utente dovrà, se richiesto da dirigente responsabile, restituire eventuali attrezzature a lui assegnate e impostare la risposta automatica sulla propria casella di posta elettronica (vedi art. 4.2.5).

Il Dirigente responsabile:

- dovrà farsi restituire eventuali dotazioni cellulari e mobili (ad es. notebook) e consegnarle al Settore che gestisce il "sistema informatico/informativo" dell'Ente. Su richiesta dell'Utente, il Dirigente potrà eventualmente autorizzare la voltura della SIM. In tal caso la comunicazione dovrà essere inviata al Settore Innovazione che provvederà ad inoltrare all'operatore di telefonia mobile la richiesta di voltura "a privato";
- potrà richiedere la disabilitazione di accesso agli applicativi gestionali (atti, protocollo, contabilità, fax server, ecc.) e ad eventuali liste di distribuzione;
- dovrà accertarsi che eventuali liste di distribuzione e le numerazioni faxserver attive sia ricevute da altri utenti ed eventualmente richiedere l'abilitazione di accesso a nuovo Utente;
- dovrà comunicare eventualmente il nuovo assegnatario della postazione di lavoro;
- dovrà comunicare la nuova assegnazione dell'interno e dell'apparato telefonico;
- potrà richiedere al Settore che gestisce il "sistema informatico/informativo" dell'Ente di impostare l'avviso di risposta automatica, nel caso in cui non sia stata impostata dall'Utente (vedi art. 4.2.5).

Si precisa che l'utenza di dominio resterà attiva al fine di consentire al dipendente l'accesso alla intranet aziendale e la consultazione del portale stipendi.

Si precisa inoltre che nel caso il dirigente di riferimento ritenga opportuno non attivare alcune delle attività dei punti elenco di cui sopra, è legittimato nella scelta prendendosene la completa responsabilità.

5.12 Comando presso altro ente

In caso di cui un dipendente vada in comando presso altro ente dovrà restituire eventuali attrezzature a lui assegnate, rendere disponibili sulle cartelle di rete eventuali files inerenti l'attività lavorativa (rendendoli disponibili ai colleghi che lo sostituiranno) ed eliminare eventuali dati personali presenti sui dispositivi in dotazione (PC, telefono, ecc.).

Il Dirigente responsabile dovrà, se lo ritiene necessario, informare il Settore che gestisce il "sistema informatico/informativo" dell'Ente richiedendo la disabilitazione di accesso agli applicativi gestionali (atti, protocollo, contabilità, fax server, ecc.) e ad eventuali liste di distribuzione come dettagliatamente indicato all'art. 5.9, oltre che farsi restituire eventuali dotazioni cellulari e mobili e consegnarle al Settore che gestisce il "sistema informatico/informativo" dell'Ente.

Il Dirigente responsabile dovrà:

- comunicare il comando al Settore che gestisce il "sistema informatico/informativo" dell'Ente;
- richiedere la disabilitazione di accesso agli applicativi gestionali (atti, protocollo, contabilità, fax server, ecc.) e ad eventuali liste di distribuzione;
- accertarsi che eventuali liste di distribuzione e le numerazioni faxserver attive sia ricevute da altri utenti ed eventualmente richiedere l'abilitazione di accesso a nuovo Utente;
- richiedere l'eliminazione della casella di posta elettronica nominativa;
- comunicare eventualmente il nuovo assegnatario della postazione di lavoro;
- comunicare la nuova assegnazione dell'interno e dell'apparato telefonico;
- farsi restituire eventuali dotazioni cellulari e mobili (ad es. notebook) e consegnarle al Settore che gestisce il "sistema informatico/informativo" dell'Ente. Su richiesta dell'Utente, il Dirigente potrà

eventualmente autorizzare la voltura della SIM. In tal caso la comunicazione dovrà essere inviata al Settore che gestisce il "sistema informatico/informativo" dell'Ente che provvederà ad inoltrare all'operatore di telefonia mobile la richiesta di voltura "a privato";

Si precisa che l'utenza di dominio resterà attiva al fine di consentire al dipendente l'accesso alla intranet aziendale e la consultazione del portale stipendi tramite citrix.

Il Dirigente responsabile, con specifica e motivata richiesta scritta, potrà richiedere una deroga a quanto sopra riportato.

Art. 6. ATTIVITÀ DI CONTROLLO E RENDICONTAZIONE

6.1 Princìpi dell'attività di controllo

I trattamenti dati che dovessero concretizzarsi durante l'attività di controllo posta in essere dalla Provincia di Brescia sono ispirati ai seguenti princìpi:

- principio di necessità, secondo il quale i sistemi e gli applicativi informatici devono ridurre al minimo l'uso di dati personali e identificativi, in relazione alle finalità perseguite;
- principio di correttezza, secondo cui i le caratteristiche essenziali dei trattamenti devono essere rese note agli utenti, in particolare perché le tecnologie dell'informazione in uso danno luogo ad operazioni sui dati che avvengono all'insaputa o senza la piena consapevolezza da parte degli utenti;
- principio di pertinenza e non eccedenza, secondo cui i dati devono essere trattati per finalità determinate, esplicite e legittime, nella misura meno invasiva possibile.

6.2 Limiti e finalità di esercizio dell'attività di controllo

Nei limiti dell'esercizio del normale potere di controllo datoriale, la Provincia verifica il corretto utilizzo delle risorse tecnologiche, di norma analizzando dati aggregati non nominativi.

Qualora dai controlli di routine, svolti su gruppi aggregati di utenti, dovessero emergere comportamenti anomali (ad esempio, un traffico dati eccessivo), ovvero al verificarsi di incidenti informatici di sicurezza (ad esempio, il diffondersi di un malware), verrà individuata un'area di rischio sulla quale focalizzare l'attenzione, e le procedure di controllo subiranno un graduale incremento, con le modalità descritte negli articoli successivi.

6.3 Modalità di svolgimento dei controlli – Navigazione Internet

Su richiesta specifica del Dirigente responsabile e/o periodicamente la Provincia di Brescia genera report statistici in forma anonima ed aggregata (per esempio in base a gruppi di utenti, categorie di siti web, frequenze di navigazione, etc.) relativi al traffico Internet.

Nel caso in cui dai report emergesse evidenza di un eccessivo e ingiustificato utilizzo della navigazione web, si attiverà la seguente procedura:

- Il Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente valuta e segnala via e-mail o comunque per iscritto l'anomalia al Dirigente responsabile.
- Contestualmente, dispone che gli amministratori di sistema raccolgano e memorizzino i log aggregati e i log nominativi relativi al personale del settore ove sia emerso il sospetto comportamento.
- Il Dirigente del settore deve comunicare al proprio personale quanto segnalato dal Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente.
- il Direttore del Settore che gestisce il "sistema informatico/informativo" dell'Ente esegue successive verifiche con periodicità ravvicinata (2-3 giorni) finalizzate all'individuazione di un eventuale riverificarsi della medesima attività.
- Solo nel caso in cui, a seguito di tali controlli, risulti il perdurare dell'attività, gli amministratori di sistema ne danno comunicazione via e-mail o comunque per iscritto al Dirigente del Settore che gestisce il "sistema informatico/informativo" dell'Ente il quale potrà richiedere l'individuazione dell'autore del

comportamento non consentito e ne darà comunicazione in forma scritta al Dirigente del settore competente.

- Il Dirigente del settore di riferimento dovrà definire quali provvedimenti adottare nei confronti dell'utente individuato.
- Qualora il Dirigente del settore di riferimento ritenga conclusa la procedura provvederà a richiedere via e-mail o comunque per iscritto al Responsabile del Settore che gestisce il "sistema informatico/informativo" dell'Ente, la distruzione dei supporti contenenti i log.

6.4 Modalità di svolgimento dei controlli – Posta Elettronica

Il sistema di posta elettronica viene costantemente monitorato ai fini di garantirne il corretto funzionamento, anche ai fini di una manutenzione proattiva.

Nel caso in cui venissero riscontrate anomalie nell'utilizzo del sistema sono previsti dei blocchi automatici sulle caselle con un utilizzo anomalo (ad esempio n. massimo di mail inviate per minuto).

In questi casi la casella viene automaticamente bloccata e non sarà più in grado di ricevere e/o inviare messaggi. In seguito alla notifica dell'anomalia gli amministratori di sistema si attiveranno per effettuare verifiche più approfondite in modo da individuare la causa del problema, anche accedendo alla casella stessa e/o contattando l'utente assegnatario della casella.

Se il problema è risolvibile tramite normale procedura di assistenza (ad esempio si riscontrano attività di spam non generate consapevolmente dall'utente) verrà inviata una segnalazione al responsabile del servizio di assistenza e la casella verrà monitorata nel corso dei 5 giorni seguenti in modo da accertare l'effettiva e definitiva risoluzione del problema.

Nel caso invece in cui si sospetti un utilizzo improprio e volontario da parte dell'utente gli amministratori ne daranno comunicazione, in forma scritta, al Direttore del Settore che gestisce il "sistema informatico/informativo" che provvederà ad informare il Dirigente responsabile dell'utente per valutare eventuali azioni da intraprendere.

6.5 Rendicontazione della telefonia fissa

Gli amministratori di sistema, a fronte di comunicazioni scritte da parte dei dirigenti di Settore, provvedono ad inibire le chiamate a numeri di telefono potenzialmente diseconomici ed effettuano tutta la configurazione del centralino IP (relativo agli interni 030 3748xxx e 030 3749xxx).

Gli amministratori di sistema possono effettuare l'estrazione dei dati delle chiamate effettuate (sempre per ragioni di servizio o su richiesta motivata da parte dei Dirigenti di settore) interrogando il data base presente sul centralino IP dell'Ente.

Periodicamente inviano la rendicontazione del traffico generato (sempre anonimizzato con le tre "xxx" sulle ultime tre cifre del numero telefonico chiamato) dai singoli interni ai dirigenti di riferimento.

6.6 Altre rendicontazioni

Ciascun Dirigente potrà richiedere al Settore che gestisce il "sistema informatico/informativo" dell'Ente la rendicontazione dei seguenti servizi:

- Asset in dotazione (PC, stampanti, telefoni cellulari, SIM, ecc.)
- Costi del traffico telefonico (fisso e mobile), sia del settore sia del singolo numero
- Dettaglio del traffico telefonico (fisso e mobile), sia del settore sia del singolo numero
- Abilitazione agli applicativi gestionali
- Abilitazioni alla navigazione internet.

Ciascun Utente potrà richiedere al Settore che gestisce il "sistema informatico/informativo" dell'Ente, esclusivamente per quanto assegnatogli, la rendicontazione dei seguenti servizi:

- Asset in dotazione (PC, stampanti, telefoni cellulari, SIM, ecc.)
- Costi del traffico telefonico (fisso e mobile)
- Dettaglio del traffico telefonico (fisso e mobile)
- Abilitazione agli applicativi gestionali
- Abilitazioni alla navigazione internet.

Art. 7. ALLEGATI

Di seguito si riportano gli allegati attualmente citati nelle “Linee guida” e che ne costituiscono parte integrante.

Considerato che trattano di procedure operative, soggette a frequenti aggiornamenti, di seguito si riportano le attuali modalità operative. L’adeguamento di tali modalità, anche sulla base degli aggiornamenti tecnici, verrà pubblicato sulla intranet nella sezione appositamente creata. Tale sezione dovrà pertanto essere costantemente consultata. In tale sezione verranno anche pubblicati eventuali nuovi allegati che andranno a illustrare nuove modalità operative e che diverranno parte integrante delle presenti “Linee Guida”.

ALLEGATO “A” - Elenco degli strumenti software utilizzati per l’attività di assistenza tecnica informatica

Gli strumenti software utilizzati dagli amministratori di sistema e dagli operatori di helpdesk per svolgere l’attività di assistenza tecnica informatica sono i seguenti:

- software TeamViewer per l’accesso al desktop Utente ed alle relative sessioni di lavoro sui personal computer in dotazione ai utenti;
- funzionalità di shadowing per l’accesso agli applicativi in uso ed alle relative sessioni di lavoro sull’infrastruttura Citrix.

ALLEGATO “B” - Istruzioni operative su come bloccare il computer e cambiare la password di dominio

Fermo restando il fatto che l’amministratore di sistema ha impostato il blocco automatico della postazione dopo 15 minuti di inattività, si elencano i passaggi da seguire per bloccare manualmente la postazione, impedendone accessi non autorizzati:

- premere contemporaneamente i tasti Ctrl + Alt + Canc (o Del – a seconda delle tastiere)
- cliccare sul pulsante “Blocca il computer”

Per modificare la password di accesso al dominio seguire invece i seguenti passaggi:

- premere contemporaneamente i tasti Ctrl + Alt + Canc
- cliccare sul pulsante “Cambio password ..”
- digitare la vecchia password e inserire due volte la nuova password (almeno 8 caratteri con numeri e lettere, deve essere diversa dalle 3 precedenti).

ALLEGATO “C” - Elenco dei software standard (per i quali è autorizzata l’installazione)

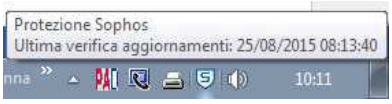
Di seguito l’elenco dei software standard installati su ogni nuova postazione di lavoro:

- Sistema operativo così come licenziato (salvo casi particolari si tratta della versione OEM dell’hardware acquistato)
- Open office

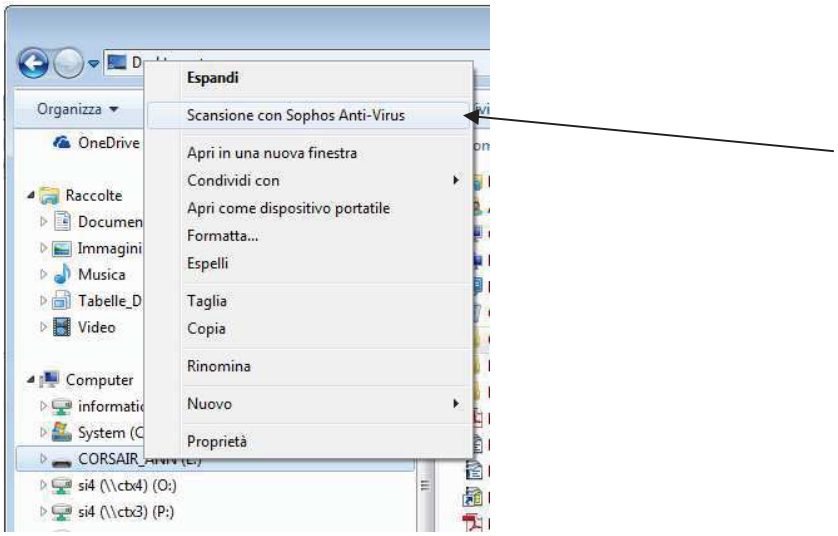
- Pdf creator
- Pdf Sam
- 7-Zip
- Dike (ed eventualmente File Protector per le firme massive)
- CRS Manager
- Java
- Vlc Mediaplayer
- Adobe Reader
- Urbiup
- I browser e i software per la gestione degli account di posta elettronica di cui rispettivamente all'Allegato F e all'Allegato G

ALLEGATO "D" - Istruzioni operative sull'utilizzo del software antivirus

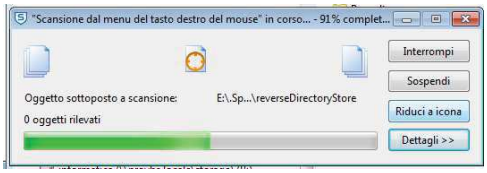
Per verificare la presenza dell'antivirus sul PC accertarsi che in basso a destra, dove c'è l'orologio, esista uno "scudetto" bianco con contorni azzurri ed una S nel mezzo  , se presente vuol dire che l'antivirus è installato.

Se lo "scudetto" ha una "X" vuol dire che c'è qualche problema di aggiornamento, altrimenti per verificare la data di aggiornamento passare con il mouse sull'icona e verrà visualizzato un fumetto contenente le informazioni. 

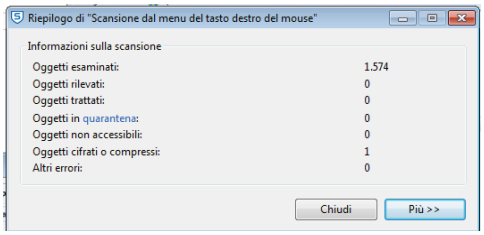
Per eseguire la scansione di dischi o chiavette usb: aprire risorse del computer e premere con il tasto destro del mouse sul disco da scansionare. Nel menù a tendina che si apre premere "Scansione con Sophos Anti-Virus" e attendere l'esito.



L'antivirus eseguirà la scansione dei file:



Al termine verrà presentato un report con l'indicazione dei file verificati ed eventualmente quelli messi in "quarantena":



ALLEGATO "E" - Lettera di assegnazione attrezzature cellulari

Alla consegna delle attrezzature cellulari l'Utente dovrà sottoscrivere una lettera nella quale vengono citate, tra le altre, le responsabilità a cui si deve attenere:

- *Prende atto che il bene è di proprietà della Provincia di Brescia e gli viene assegnato per un uso strettamente pertinente alle mansioni svolte e alle funzioni del suo ufficio; si impegna pertanto a custodirlo con la massima diligenza e a restituirlo prontamente al Settore Innovazione alla cessazione delle circostanze che ne hanno reso necessaria l'assegnazione ovvero su richiesta del Dirigente che ne ha disposto l'assegnazione.*
- *Si impegna a rimborsare alla Provincia ogni ed eventuale chiamata eseguita a titolo strettamente personale.*

Nel caso in cui l'attrezzatura assegnata sia configurata per la gestione di dati aziendali (ad esempio casella di posta elettronica) dovrà sottoscrivere anche i seguenti impegni:

Prende atto che l'apparato viene gestito in modalità centralizzata (quindi l'amministratore di sistema gestirà il dispositivo da postazione remota) e pertanto autorizza fin da ora a:

- *procedere alla cancellazione completa dei dati presenti sul dispositivo in caso di furto o smarrimento;*
- *resettare la password (passcode) per bloccare l'accesso al dispositivo;*
- *inventariare il dispositivo sia per quanto riguarda i dati hardware, sia per quanto riguarda le statistiche di utilizzo, sia per quanto attiene le informazioni Utente (ad es. account in uso, ecc.);*
- *aggiungere o rimuovere account e/o restrizioni nell'utilizzo del dispositivo;*
- *installare e gestire le applicazioni di servizio;*
- *procedere alla geolocalizzazione del dispositivo su richiesta dell'utilizzatore e/o del Dirigente che ne ha disposto l'assegnazione, ovvero per necessità di recupero in seguito a furto o smarrimento.*

Si impegna a:

- *eseguire backup periodici dei dati personali memorizzati sul dispositivo;*
- *per ragioni di sicurezza personalizzare al primo accesso la password (modificandola con periodicità);*

- *non rimuovere le applicazioni di servizio autoinstallate e/o modificare le configurazioni standard impostate dall'amministratore di sistema;*
- *non eseguire procedure che permettano di installare applicazioni e pacchetti alternativi a quelli ufficiali previsti dall'Apple Store ovvero dal Play Store (eseguire ad esempio jailbreak sugli apparati IOS).*

Quanto sopra riportato è riferito alla data di pubblicazione delle presenti "Linee Guida" e pertanto potrebbe essere soggetto ad aggiornamenti.

ALLEGATO "F" - Elenco dei programmi a disposizione per la navigazione in internet (browser)

Avendo riscontrato che non tutti i siti e/o gli applicativi sono perfettamente compatibili con i diversi browser e le loro differenti versioni, si stabilisce che sulle postazioni possano essere installati più browser tra quelli più diffusi:

- Microsoft Internet Explorer;
- Mozilla Firefox;
- Google Chrome;
- Safari;
- Opera.

ALLEGATO "G" - Elenco dei programmi a disposizione per la posta elettronica e dimensione massima delle caselle

Per la consultazione della posta elettronica sul PC è possibile utilizzare:

- Microsoft Outlook;
- Office 365 on line.

La dimensione massima delle caselle sul server è 1 TeraByte.

ALLEGATO "H" - Categorie di filtraggio dei siti web

Le categorie sotto elencate sono parzialmente soggette a filtro web in base ad algoritmi gestiti dall'applaiance Fortigate.

- Local Categories
- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest – Personal
- General Interest – Buisness
- Unrated

ALLEGATO "I" - Istruzioni operative per la cancellazione della cronologia delle pagine web visitate, della memoria cache e dei cookies

Le modalità da seguire variano in base al programma utilizzato:

- Internet Explorer: cliccare su strumenti o icona ingranaggio, opzioni internet, alla voce cronologia premere il tasto "Elimina" e spuntare le caselle interessate per eliminare le varie cache.
- Google Chrome: premere le tre lineette orizzontali in alto a destra, impostazioni, cliccare su "Mostra impostazioni avanzate…", cliccare sul pulsante "Cancella dati di navigazione…" e spuntare le caselle interessate per eliminare le varie cache.
- Mozilla Firefox: premere le tre lineette orizzontali in alto a destra, opzioni, cliccare sulla casella "Privacy", cliccare su "cancellare la cronologia recente", nel menù a tendina selezionare l'intervallo di tempo da cancellare e premere il tasto "Cancella adesso".

ALLEGATO "J" - Istruzioni operative sull'utilizzo del messaggio di assenza dall'ufficio (fuori sede)

Per impostare un messaggio procedere nel seguente modo, a seconda del programma utilizzato per la consultazione dell'account di posta:

- Outlook: cliccare su "Strumenti", Regole fuori sede, spuntare la voce "Invia messaggi Fuori sede – Risposta automatica", selezionare la data di inizio e fine e scrivere un messaggio nel campo "Interni all'organizzazione" e nel campo "Esterni all'organizzazione", cliccare su ok per chiudere.
- Outlook 365 on-line: andare alla pagina https://login.microsoftonline.com inserire le credenziali di dominio, cliccare su posta, cliccare sull'icona dell'ingranaggio in alto a destra, cliccare su risposte automatiche e spuntare la voce "Invia risposte automatiche", selezionare la data di inizio e fine, scrivere il messaggio e premere sul tasto "OK" in alto.

ALLEGATO "K" - Avvertimento automatico per le e-mail (firma in calce ai messaggi)

Per impostare la propria firma in calce a tutti i messaggi procedere nel seguente modo, a seconda del programma utilizzato per la consultazione dell'account di posta:

- Outlook: cliccare su strumenti, opzioni, Formato posta, Firma, cliccare su nuovo e digitare un nome di riconoscimento, premere ok, nel campo bianco scrivere la firma e selezionare se inserirla in automatico nei nuovi messaggi e nelle risposte, premere ok due volte per salvare.
- Outlook 365/2013: cliccare su file in alto a destra, opzioni, posta, firme, cliccare su nuova e digitare un nome di riconoscimento, premere ok, nel campo bianco scrivere la firma (anche su più righe – si suggerisce di inserire nominativo, settore, indirizzo, recapito telefonico e pec) e selezionare se inserirla in automatico nei nuovi messaggi e nelle risposte, premere ok due volte per salvare.

Si rammenta che in calce a tutte le mail inviate viene apposto automaticamente un messaggio relativo alla riservatezza dei dati contenuti nel messaggio stesso. Attualmente è il seguente:

Ai sensi e per gli effetti delle disposizioni vigenti in materia di tutela della riservatezza personale (D.lgs 196/2003), questa mail e' destinata unicamente alle persone sopra indicate e le informazioni in essa contenute sono da considerarsi strettamente riservate. E' proibito leggere, copiare, usare o diffondere il

contenuto della presente mail senza autorizzazione. Se avete ricevuto questa mail per errore, siete pregati di rispedire la stessa al mittente. Questo indirizzo di posta elettronica e' riservato esclusivamente a comunicazioni istituzionali della Provincia di Brescia.

ALLEGATO “L” - Profili di navigazione internet

Di seguito si elencano i diversi profili di navigazione attivabili su ciascun Utente:

- Internet livello 1 - navigazione di base
- Internet livello 2 – abilitazioni del profilo 1 con l’aggiunta dei siti di file sharing
- Internet livello 3 - abilitazioni del profilo 2 con l’aggiunta dei social network
- Internet livello 4 - abilitazioni del profilo 3 con l’aggiunta dei siti di video streaming
- Internet livello 5 - abilitazioni del profilo 4 con l’aggiunta di particolari abilitazioni di accesso ai siti che utilizzano particolari porte “non standard”. Viene rilasciato solo su specifica e motivata richiesta
- Internet livello S - abilitato ai soli amministratori di sistema