Allegato 14
al Manuale di Gestione del Protocollo informatico, dei flussi documentali e degli archivi del Comune di Stresa

Piano per la Sicurezza

Riferimenti normativi

Il 'piano per la sicurezza informatica' riporta le misure minime di sicurezza, organizzative e tecnologiche, messe in atto dal Comune di Stresa.

Il presente documento è il Piano per la Sicurezza ai sensi del Codice dell'Amministrazione Digitale (D.L.gs n. 82 del 7 marzo del 2005), del testo Unico 445/200 e del D.Lgs. 196/2003.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

SICUREZZA

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dall'applicazione informatica adottata dall'Ente.

Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale.

Il presente capitolo riporta le misure di sicurezza adottate specifiche per l'infrastruttura di protocollo informatico anche in relazione alle norme sulla protezione dei dati personali.

Obiettivi

La politica in merito alla sicurezza di questo Ente è finalizzata a assicurare che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo,mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita,anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

A tale fine l'Ente definisce:

1. le politiche generali e particolari di sicurezza da adottare all'interno della AOO;

2. le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;

3. gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, *di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali*, in caso di trattamento di dati personali;

4. i piani specifici di formazione degli addetti;

5. le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il Responsabile della gestione documentale ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza prestabilita durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;

- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad *es. separazione della parte anagrafica da quella "sensibile*") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

Credenziali di accesso al sistema documentale

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di gestione documentale e protocollo informatico nel rispetto di modalità prestabilite.
Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).
Gli utenti del programma di gestione documentale e protocollo, in base alle rispettive competenze, dispongono di autorizzazioni di accesso differenziate.
Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l'identificazione dell'utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password);
- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e workflow effettuabili alle sole funzioni necessarie.

La visibilità normalmente attribuita ad un utente si limita alla documentazione relativa ai servizi di competenza. La visibilità su altri documenti può essere attribuita dal responsabile della pratica o del procedimento.
L'accesso diretto alla banca dati, l'inserimento di nuovi utenti, la modifica dei diritti e le impostazioni sui documenti sono consentiti esclusivamente agli amministratori del sistema.
I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Gli accessi esterni a documenti, dati e informazioni non divulgabili sono subordinati alla registrazione sul sistema e al possesso di apposite credenziali, rilasciate previa identificazione diretta da parte di un dipendente abilitato.
Gli accessi esterni a documenti, dati e informazioni divulgabili sono consentiti anche senza autenticazione all'accesso, garantendo comunque il diritto alla riservatezza e all'oblio, e la tutela dei dati personali in conformità alle disposizioni vigenti.
Gli accessi esterni vengono di norma gestiti attraverso il sito web dell'Ente. I dati in libera consultazione vengono esposti in formato aperto (con dovute eccezioni, indotte anche da considerazioni di carattere tecnico, organizzativo o gestionale) che ne consentano il riutilizzo.

Sicurezza nella formazione dei documenti
Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti sono prodotti con l'ausilio dell'applicativo specificato nell'allegato 7 che possiede i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF/A, XML, TIFF.
I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF/A, XML e TIFF) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici.
L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Trasmissione ed interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale l'amministrazione, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Definizioni

Trattamento di dati: si intende, qualunque operazione o complesso di operazioni, effettuati con l'ausilio di strumenti elettronici, concernenti: la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati (art.4 del D.Lgs. 196/2003).

Dati sensibili: dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Dati giudiziari: dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Titolare: persona fisica o giuridica o altro organismo cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, compreso il profilo della sicurezza.

Responsabile del trattamento: persona fisica o giuridica preposta dal titolare al trattamento dei dati personali.

Incaricato: persona fisica identificata tramite apposita nomina del Responsabile del trattamento che esegue le operazioni di trattamento. La nomina degli incaricati del trattamento rientra tra le competenze dei predetti Responsabili del trattamento.

Addetti alla custodia delle parole chiave: persone incaricate della custodia delle parole chiave di accesso ad informazioni o di accedere alle stesse.

Amministratori di sistema: soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo e/o di gestione dei data base e di consentirne l'utilizzazione. Sono individuati nei Dirigenti in capo ai quali è configurabile la gestione e la responsabilità di un sistema informatico ovvero nei soggetti esterni incaricati della gestione del sistema informatico.

Incaricati della manutenzione: persone addette alla manutenzione dell'hardware, del software applicativo e del software di base degli elaboratori sui quali sono memorizzati i dati personali.

PDL: postazione di lavoro.

HOST – Server: con HOST si identificano le macchine fisiche che ospitano i Server, ovvero le macchine virtuali che svolgono funzioni informatiche od ospitano gli applicativi software.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Introduzione

L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è anche quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, i software applicativi, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, di gestione documentale, di protocollazione e conservazione digitale a norma etc.

Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori.

È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

Scopo

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione in ogni suo aspetto. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

Ambito di applicazione

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, stagisti, ...), includendo tutto il personale affiliato con terze parti. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

Politiche di sicurezza

1. Indirizzi utilizzazione strumenti informatici e indirizzi generali relativi all'utilizzazione di internet. (Allegato 1).

2. Specifiche di Backup attuate nell'ente (Allegato 2).

3. Studio di fattibilità tecnica relativo al piano di continuità operativa e disaster recovery (Allegato 3)

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Allegato 1)

Indirizzi utilizzazione strumenti informatici
e indirizzi generali relativi all'utilizzazione di internet

Principi generali

1. Il presente disciplinare è stato approvato con deliberazione della Giunta Comunale N. 197 del 22.10.2010 (Regolamento sul funzionamento degli uffici e dei servizi, articolo 156 – Allegato Q).

2. La violazione del presente disciplinare potrà comportare l'applicazione delle sanzioni disciplinari contemplate dal Contratto collettivo nazionale di lavoro applicabile, nel rispetto dei principi di gradualità e proporzionalità, nonché delle altre misure di tutela del caso.

Premessa.

La possibilità di usufruire dei mezzi telematici messi a disposizione dal Comune, rende necessaria la regolamentazione dell'utilizzo di questa risorsa al fine di garantire un servizio corretto, sicuro e funzionale.

Inoltre la diffusione di Internet rende sempre più critico il problema della navigazione protetta.

E' necessario stabilire delle regole alle quali tutto il personale è tenuto a rispettare.

Principi generali

Gli strumenti informatici forniti al personale dipendente devono essere utilizzati esclusivamente per lo svolgimento del lavoro assegnato con modalità e comportamenti adeguati ai compiti ed alle responsabilità dei dipendenti pubblici, rispettando i comuni principi ed etici, nonché la *privacy e* la segretezza dei dati trattati.

Ciascun dipendente è responsabile per l'utilizzo da parte di terzi, anche se conosciuti o affini, degli strumenti informatici a lui affidati.

Per strumenti informatici si intendono:

personal computer fissi o portatili, videoterminali, stampanti locali o di rete, i prodotti software regolarmente licenziati, palmari, cellulari o altri dispositivi di telecomunicazione, le relative periferiche nonché tutta l'infrastruttura logica e fisica che permette l'interconnessione delle postazioni di lavoro al fine di agevolare la trasmissione di dati.

Norme di comportamento.

Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio Responsabile di servizio.

L'utilizzo degli strumenti informatici al di fuori dell'orario di servizio è consentito solo previa autorizzazione del proprio Responsabile.

Il personale è tenuto ad osservare le direttive del Responsabile dei sistemi informativi volte a garantire il corretto funzionamento delle procedure di backup.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

I dati, documenti o file di qualsiasi genere (creati o modificati attraverso le applicazioni di produttività individuale – es. office o open office) devono essere salvati solo sui supporti appositamente destinati sul NAS server (unità di rete con cartelle dedicate agli uffici o personali).
Si intendono tutti i file creati utilizzando word, excel, powerpoint, access o prodotti simili (es. open office etc.).
Tale disposizione può essere derogata, su disposizione del Responsabile di servizio, solo per motivi tecnici.
Durante le sessioni di lavoro gli strumenti elettronici non possono essere lasciati incustoditi e accessibili a terzi; pertanto, ogni qualvolta il dipendente si allontani o si assenti dalla postazione di lavoro usata per il trattamento dei dati, è tenuto a chiudere la sessione, oppure a rendere inaccessibile a terzi (ad esempio mediante l'utilizzo del salva schermo dotato di password, o eventuale estrazione dell'hardware USB di autenticazione) la propria postazione di lavoro.
Si possono effettuare copie di dati su supporti rimovibili (es. dischetti CD, DVD, chiavi USB) solo se autorizzati da parte del proprio Responsabile del servizio.
Qualora sulle copie venissero trasferiti dati personali, gli stessi vanno utilizzati con le modalità previste dalla legge, e secondo il principio di necessità.
Al termine del trattamento sarà cura del dipendente distruggere o rendere inutilizzabili i supporti rimovibili eventualmente utilizzati.
I supporti rimovibili contenenti dati sensibili o giudiziari, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri dipendenti, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e in alcun modo ricostruibili.
Per rispetto delle norme che regolano la tutela giuridica del software e per la necessità di garantire integrità e stabilità delle applicazioni installate sul personal computer stesso non è consentito:
1. alterare, rimuovere o danneggiare le configurazioni del software e dell'hardware dei personal computer ;
2. installare e utilizzare programmi informatici che non siano stati ufficialmente forniti o acquistati dal Comune;
3. installare giochi, screens vers, client chat etc;
4. installare dispositivi di comunicazione (*modem*) se non con l'autorizzazione espressa del Responsabile dei Sistemi informatici;
5. installare o connettere periferiche proprie;
6. scaricare da internet o da supporto magnetico proveniente dall'esterno file di provenienza sconosciuta senza farli sottoporre ad opportuno controllo;
7. divulgare informazioni tecniche relative alla struttura informatica comunale che possano pregiudicare la sicurezza della stessa.
E' inoltre espressamente vietato:
1. utilizzare gli strumenti informatici comunali al fine di custodire, fare circolare o promuovere materiale pubblicitario personale, codice maligno *(virus, trojan horses, programmi pirata)* o altre porzioni di codice maligno e/o altro materiale non autorizzato.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

2. copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto d'autore (documenti, *files* musicali, immagini, filmati e simili) di cui l'ente non abbia acquisito i diritti.
3. utilizzare la strumentazione informatica per la realizzazione, redazione, memorizzazione e spedizione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e politica.
Il Responsabile del settore sistemi informativi o personale dallo stesso autorizzato, può in ogni momento, previo congruo avviso all'interessato e per fini meramente diagnostici e tecnici, verificare sul computer del dipendente il rispetto delle regole precedenti.

Norme per l'autenticazione informatica (Questa parte richiama le disposizioni della vigente normativa in tema di trattamento dei dati personali e relative misure minime di sicurezza (art. 33 del D. Lgs. n. 196/2003).
Il trattamento di dati personali sul computer comunale è consentito, all'interno del Comune,
solamente agli incaricati dotati di personali credenziali di autenticazione ovvero del codice per l'identificazione dell'utente (user id) associato a una parola chiave (password).
La parola chiave è riservata, deve essere conosciuta solamente dal dipendente che non deve, in alcun caso, comunicare a terzi.
Ogni dispositivo hardware di autenticazione (chiave hardware) deve rimanere in possesso e uso esclusivo del dipendente.
Il dispositivo è di proprietà del Comune, non può essere né prestato né ceduto a terzi, neppure temporaneamente.
In caso di allontanamento, anche solo temporaneo, dall'elaboratore, il dispositivo deve essere estratto e custodito.
La parola chiave deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili al dipendente.
La parola chiave deve essere modificata dal dipendente al primo utilizzo e, successivamente, almeno ogni tre mesi.
A tal fine il Responsabile sistemi informativi adotta le misure tecniche necessarie affinché la procedura di modifica della parola chiave venga proposta automaticamente all'utente.
Le credenziali e la password possono essere attribuite unicamente al personale autorizzato dal Comune e le stesse possono essere assegnate unicamente al personale autorizzato.
In caso di assenza del dipendente, e contingente necessità indispensabile e indifferibile di intervenire per esclusive necessità di operatività e di sicurezza del sistema, il Responsabile del servizio può assicurare la disponibilità di dati e degli strumenti informatici richiedendo al Responsabile dei sistemi informativi l'attribuzione di nuove credenziali di accesso ed eventuale assegnazione delle credenziali di un nuovo temporaneo incaricato sostitutivo.
Al suo ritorno, il dipendente verrà informato tempestivamente circa l'intervento effettuato.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Norme per il rischio di intrusione e *antivirus*
Al fine di proteggere i dati dal rischio di accesso abusivo e dall'azione dannosa di programmi (ad esempio v*irus),* il Responsabile dei sistemi informativi predispone a livello centralizzato, adeguati strumenti elettronici nonché il loro aggiornamento secondo le modalità previste dalla legge.
Il personale è tenuto a segnalare ogni malfunzionamento degli strumenti dei programmi antivirus, ed affini e per nessun motivo è autorizzato a disattivarli**.**

Regole per la navigazione su internet e posta elettronica.
La rete Internet è una risorsa messa a disposizione del personale come fonte di informazione per finalità di documentazione, ricerca e studio utili per lo svolgimento del proprio lavoro.
Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete comunale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica *(firewall, antivirus,* etc.).
Tutto il personale può connettersi alla rete Internet tramite gli strumenti a disposizione.
Tenuto presente il recente provvedimento del Garante della Privacy, ed evidenziato che dal sito web si possono trarre informazioni anche sensibili sui dipendenti e i messaggi di posta elettronica possono avere contenuti a carattere privato, e per prevenire usi arbitrari degli strumenti informatici aziendali e la lesione della riservatezza dei lavoratori, si informa il personale, con chiarezza e in modo dettagliato, sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli.
Per quel che riguarda la **navigazione su internet**, vengono esplicitate le attività per le quali non è consentito:
1. registrarsi a siti, *mailing-list, forum,* bacheche elettroniche o altri servizi *on line senza* specifica autorizzazione in tal senso da parte del proprio Responsabile del servizio;
2. utilizzare applicazioni "chat – line".
3. scaricare *software, a*nche se gratuito, prelevato da siti Internet, ad eccezione di quanto previsto per motivi di lavoro;
4. installare o utilizzare *software "peer to peer ",* finalizzato allo scambio e alla diffusione tramite la rete Internet, di materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore;
5. prelevare da Internet e/o archiviare sul proprio elaboratore, ovvero sulle risorse di rete condivise, documenti informatici (testo, audio, immagini, filmati, etc.) di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica appartenenza sindacale o politica o che comunque possano risultare offensivi della dignità umana.
6. diffondere attraverso Internet materiale commerciale o pubblicitario non richiesto
7. trasmettere via Internet *virus,* worms, *trojan - horses* o altro codice maligno, noto per arrecare danni e malfunzionamenti ai sistemi informatici.
8. prelevare da Internet, ovvero inviare tramite Internet, dati o altre risorse informatiche per scopi non consentiti dalle norme vigenti.
9. fornire a soggetti non autorizzati l'accesso alla connessione Internet comunale;
10. utilizzare la connessione Internet al fine di recare danno o disturbo a terzi;

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

11. effettuare transazioni commerciali e/o finanziarie di natura personale, ivi comprese operazioni di *remote banking, a*cquisti *on line* e simili, salvo specifica autorizzazione.

Per quel che riguarda la **posta elettronica** il Comune:
a) potrà mettere, su apposita richiesta e compatibilmente con gli aspetti tecnici, a disposizione anche indirizzi condivisi tra più lavoratori (ad esempio: info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
b) potrà attribuire, su richiesta del dipendente interessato e compatibilmente con gli aspetti tecnici, un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
c) potrà prevedere, in caso di assenza del dipendente, messaggi di risposta automatica con le coordinate di altri dipendenti cui rivolgersi;
d) potrà consentire il dipendente di delegare un altro dipendente (fiduciario) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del dipendente interessato e di improrogabili necessità legate all'attività lavorativa.
Qualora queste misure preventive non fossero sufficienti a evitare comportamenti anomali, gli eventuali controlli da parte del Responsabile dei sistemi informatici saranno effettuati con gradualità; in prima battuta si effettueranno verifiche di ufficio in modo da invitare il Responsabile del Servizio a richiamare il personale assegnato all'osservanza delle regole di cui sopra e se si ripetesse l'anomalia, si passerà a controlli su base individuale.

Norma finale.
La presente direttiva sarà consegnata a ciascun dipendente del Comune di Stresa, che è tenuto a firmare per ricevuta.
Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali
Informatiche comunali, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni ".
La violazione da parte dei lavoratori dei principi e delle norme contenute nel presente regolamento costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, il Responsabile del servizio gestione risorse umane, previo espletamento di procedimento disciplinare, può procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038

Allegato 2)
Specifiche di backup

Procedura:
i seguenti elaboratori di tipo server sono sottoposti a procedura di backup gestita da una procedura automatizzata dedicata.
Server con sistemi operativi Microsoft (MS 2k3-2k12):
server1
server2
Ml350g3
Applicazione di backup e server coinvolti:
La procedura automatica è gestita dall'applicativo Open Source Cobian Backup
Supporti di backup:
i backup vengono eseguiti utilizzando supporti esterni (disco USB) e tra i due server
Tipi di backup:
le sessioni di backup si distinguono nei tipi:
totali detti FULL ;
incrementali detti INCn.
Periodicità delle sessioni di backup e durata della conservazione:
I backup avvengono giornalmente in ore notturne e riguardano tutti archivi, i backup completi vengono conservati per 1 mese
Cosa viene salvato nei backup:
contenuto di tutti i file system gestiti dagli elaboratori;
tutti i db attivi contenuti in ogni istanza MS SQL Server presente sugli elaboratori;
Modalità di controllo:
Al termine di ogni processo di backup il sistema invia una mail con il log dell'operazione effettuata contenente esito dell'operazione ed eventuali errori nell'esecuzione.
Evoluzione:
E' opportuno attivare procedure di backup bisettimanali su supporti che vengano custoditi in sede separata.

Allegato 3)
Studio di fattibilità tecnica relativo al piano di continuità operativa e disaster recovery

Il Comune di Stresa dovrà dotarsi di uno studio di fattibilità tecnica per la Continuità Operativa ed il Disaster Recovery, con tempistica in fase di analisi e programmazione.

28838 – Stresa (VB), piazza Matteotti civ. 6
tel. 0323 - 939111
protocollo@cert.comunestresa.it * info@comune.stresa.vb.it
Codice Fiscale 00201600038