Holding Ferrara Servizi Srl e le sue controllate

LINEE GUIDA PER IL TRATTAMENTO SICURO DEI DATI E PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI

Versione del documento

N°	Data	Descrizione	Emesso	Verificato	Approvato
1.0	13/12/2018	Prima emissione	13/12/2018	13/12/2018	13/12/2018

Sommario

INTRODUZIONE

L'uso improprio degli strumenti che **Holding Ferrara Servizi Srl e le sue controllate** mettono a disposizione per il trattamento dei dati e delle informazioni, oltre ad arrecare un danno in termini di maggiori costi e possibili perdite di continuità del servizio, può nuocere alle stesse da un punto di vista della reputazione e condurre a procedimenti legali con sanzioni di tipo amministrativo e penale.
Poiché la sicurezza dei dati non dipende solo da aspetti tecnici, ma anche, se non principalmente, da quelli organizzativi e comportamentali, tutti i lavoratori[1] devono considerarla una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione.
Anche la vigente normativa in materia di protezione dei dati personali e i Provvedimenti del Garante Privacy impongono, per procedere ad ogni trattamento dei dati personali, l'adozione e il rispetto di certi criteri guida nel trattamento dei dati.

Quale complemento e integrazione della sicurezza, è necessario quindi adottare e diffondere una politica aziendale trasparente in cui siano esplicitati i limiti di utilizzo delle risorse assegnate ai lavoratori per lo svolgimento delle mansioni lavorative nonché le regole comportamentali da osservare per trattare in modo sicuro sia i dati informatici che quelli cartacei.
L'adozione di queste politiche viene fatta nell'intento di:

- provvedere ad un servizio continuativo nell'interesse dell'Azienda
- salvaguardare la riservatezza delle informazioni e dei dati
- tutelarsi da potenziali responsabilità legali
- proteggere il buon nome e l'immagine dell'azienda
- proteggere gli investimenti effettuati
- evitare problemi di sicurezza informando e incentivando i comportamenti corretti
- garantire la massima efficienza delle risorse informatiche e del loro utilizzo
- contribuire al rispetto delle norme sul trattamento di dati personali

FINALITÀ DEL DOCUMENTO

Questo documento viene incontro alla necessità di disciplinare il trattamento di dati personali e le condizioni per il corretto utilizzo dei beni aziendali in applicazione dei principi di cui alla vigente normativa in materia di protezione dei dati personali e delle indicazioni del Provvedimento a carattere generale - 01 marzo 2007 - "Linee guida del Garante per posta elettronica e Internet".

Con il presente documento **Holding Ferrara Servizi Srl e le sue controllate** intendono contribuire alla massima diffusione della cultura della sicurezza per evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla riservatezza-sicurezza nel trattamento dei dati.

Il presente documento regola pertanto sia l'utilizzo degli strumenti per il trattamento dei dati cartacei, sia l'utilizzo del Sistema Informativo Aziendale costituito dal complesso delle postazioni di lavoro (terminale, pc desktop, pc portatile, smartphone), delle periferiche, dei server e di qualsiasi risorsa hardware o software resa disponibile dalla **Holding Ferrara Servizi Srl e/o dalle sue controllate** per l'uso da parte dei propri lavoratori.

[1] *Ai fini della corretta applicazione delle presenti linee guida, si intende per «lavoratore» una persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione aziendale, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. Al lavoratore così definito è equiparato: il soggetto beneficiario delle iniziative di tirocini formativi e di orientamento; l'allievo degli istituti di istruzione ed universitari impegnati in tirocini curriculari, stage o periodi di alternanza scuola lavoro, e il lavoratore somministrato dipendente da società interinale.*

DEFINIZIONI

1. “trattamento”, qualunque operazione o complesso di operazioni, effettuati anche senza 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, anche se non registrati in una banca di dati;
2. “dato personale”, qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
3. “dati c.d. identificativi”, i dati personali che permettono l'identificazione diretta dell'interessato (nome, cognome, codice fiscale, indirizzo e-mail...);
4. “dati c.d. sensibili”, i 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, i dati personali idonei a rivelare lo stato di salute e la vita sessuale, i dati genetici, i dati biometrici;
5. “titolare”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
6. “c.d. incaricati”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
7. “interessato”, la persona fisica cui si riferiscono i dati personali;
8. “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
9. “diffusione”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
10. "Garante Privacy", l'autorità per la Protezione dei dati personali con compiti di vigilanza, indirizzo, informazione, promozione, consultazione e dotata di poteri ispettivi e sanzionatori.

REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell’interessato.

Qualunque trattamento di dati personali da parte della **Holding Ferrara Servizi Srl e delle sue controllate** è consentito soltanto per lo svolgimento delle attività aziendali.

CIRCOLAZIONE INTERNA E COMUNICAZIONE DEI DATI

Circolazione interna dei dati

L’accesso ai dati personali da parte dei lavoratori della **Holding Ferrara Servizi Srl e delle sue controllate** comunque limitato ai casi in cui sia necessario al perseguimento dei fini aziendali, è ispirato al principio della libera circolazione delle informazioni all’interno dell’Azienda.
Ogni richiesta d’accesso ai dati personali da parte dei lavoratori della **Holding Ferrara Servizi Srl e/o delle sue controllate**, purché connessa con lo svolgimento dell’attività inerente alla specifica funzione del richiedente (ambito del trattamento), deve essere soddisfatta in via diretta, senza formalità, nella misura necessaria al perseguimento dell’interesse aziendale.

Laddove la richiesta da parte dei lavoratori della **Holding Ferrara Servizi Srl e delle sue controllate** fosse finalizzata ad un utilizzo ulteriore e/o diverso dei dati, sarà necessario, da parte di questi soggetti, presentare una richiesta scritta e motivata.

Chi richiede i dati, chi li riceve, chi li tratta e chi ne ha notizia è vincolato al rispetto del segreto d'ufficio. La responsabilità, anche penale, prevista dal D.Lgs. 196 del 30 giugno 2003 per l'uso non corretto dei dati personali conosciuti resta a carico della singola persona cui l'uso illegittimo si riferisca.

Comunicazione dei dati

L'utilizzo dei dati personali deve avvenire in base al principio del "*need to know*" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati possono essere comunicati all'esterno esclusivamente ai soggetti e nei modi indicati nell'informativa sul trattamento dei dati rilasciata dalla **Holding Ferrara Servizi Srl e/o dalle sue controllate**.
La comunicazione di dati personali da parte della **Holding Ferrara Servizi Srl e delle sue controllate** è effettuata in esecuzione di obblighi di legge e per le sole finalità indicate nell'informativa per il trattamento dei dati personali rilasciata dalla **Holding Ferrara Servizi Srl e/o dalle sue controllate**.
Una volta verificata la sussistenza di tali prerequisiti, prima di effettuare la comunicazione dei dati occorrerà in ogni caso:

- accertarsi dell'identità del soggetto a cui i dati vengono comunicati
- verificare l'esattezza dei dati comunicati.

Non è consentito fornire informazioni telefoniche contenenti dati personali a chicchessia, ivi comprese amministrazioni pubbliche o autorità giudiziarie.

Particolare attenzione va riposta in caso di domande/interviste telefoniche cui si raccomanda di non rispondere oppure di rispondere solo dopo ricevimento di nota informativa scritta (lettera, fax, e-mail) che consenta di verificare l'identità e il titolo del richiedente nonché le finalità della richiesta.

Massima cautela deve essere applicata anche nell'invio di informazioni a mezzo fax, pertanto occorrerà prestare attenzione a:

- digitare correttamente il numero di fax del destinatario;
- controllare l'esattezza del numero prima di inviare il documento;
- stampare il rapporto di trasmissione verificando (ove ricevuto) l'identificativo del numero chiamato.

SICUREZZA FISICA

La sicurezza fisica è l'insieme delle misure di protezione fissate per impedire l'accesso fisico di terzi non autorizzati ai dati, cartacei o informatici.

E' responsabilità dell'utente:

- provvedere alla custodia delle apparecchiature in dotazione utilizzandole in modo adeguato, eventuali danneggiamenti, smarrimenti o furti dovranno essere comunicati immediatamente alla Direzione;
- mantenere i propri supporti di memorizzazione (CD, DVD, floppy, device USB, ecc.) in luogo appropriato e possibilmente non in vista quando non sono utilizzati; se contengono dati riservati o personali ai sensi delle leggi vigenti in materia di privacy, dovranno essere custoditi in armadi o cassetti chiusi a chiave;
- tenere lontani i supporti di memorizzazione da rischi ambientali come calore eccessivo, luce solare diretta e campi magnetici;
- evitare di esporre l'hardware a condizioni estreme di umidità e/o temperatura o a contatti con liquidi, fumo ecc.;
- tener conto dei rischi derivanti da eventi straordinari dovuti a cause naturali (come incendi, allagamenti, ecc.);
- procedere a spostamenti, disconnessioni, reinstallazioni, ecc. delle apparecchiature in dotazione solo con l'autorizzazione della Direzione;
- trasportare fuori dallo stabilimento le apparecchiature portatili condivise con altri utenti (es.: un portatile non in dotazione stabile) solo con il consenso del proprio diretto superiore;
- conservare documenti contenenti dati personali in locali non accessibili a terzi non autorizzati;
- assicurarsi che l'accesso alle aree ove sono custoditi dati sia controllato visivamente da qualcuno o che le stesse aree siano chiuse a chiave;
- fare attendere soggetti terzi in luoghi in cui non siano presenti informazioni riservate o dati personali;
- chiudere le finestre e le porte al termine delle attività lavorative o comunque quando gli uffici non sono presidiati;

- riporre i documenti ed effettuare la disconnessione del proprio PC o attivarne il salvaschermo con password quando è necessario allontanarsi dalla scrivania.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

E' responsabilità dell'utente seguire le istruzioni di seguito esposte.

Istruzioni per la custodia di dati personali

- gli atti e i documenti contenenti dati personali devono essere controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione;
- al termine delle operazioni di trattamento riporre gli atti e i documenti negli archivi;
- gli atti e i documenti contenenti dati personali sensibili o comunque riservati per l'Azienda devono essere conservati in armadi o cassetti dotati di serratura;
- i dati idonei a rivelare lo stato di salute devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;
- non lasciare sparsi sulle scrivanie o appoggiati su ripiani o in luoghi in cui siano visibili a terzi non autorizzati (che possono venirne a conoscenza e divulgarli) atti e documenti cartacei (anche lettere o comunicazioni pervenute tramite la posta o a mezzo telefax);
- fotocopie o copie di documenti devono essere custodite con le stesse modalità dei documenti originali;
- in caso di utilizzo di stampanti condivise o collocate in spazi comuni, i documenti cartacei dovranno essere prelevati immediatamente dopo la stampa.

Istruzioni per la distruzione di dati personali

Qualora sia necessario distruggere i documenti contenti dati personali, la distruzione definitiva deve avvenire in modo controllato ed in modalità tale da assicurare il non riutilizzo dei dati (ad esempio utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, essere sminuzzati in modo da non essere più ricomponibili).
I supporti rimovibili contenenti dati sensibili se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Istruzioni per il trattamento di dati sensibili

L'archiviazione dei documenti cartacei contenenti dati sensibili deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Sicurezza logica

La sicurezza logica è l'insieme delle misure di protezione stabilite per assicurare che gli accessi ai sistemi informativi avvengano secondo modalità predefinite, tali da garantire un elevato livello di robustezza ed affidabilità.
A tal scopo è necessario identificare gli utenti che accedono ai sistemi informatici utilizzati per il trattamento dei dati.

Accesso ai dati sul Sistema Informativo

Gli utenti possono accedere ai dati personali presenti sul *Sistema Informativo* mediante dispositivi informatici previa procedura di autenticazione. Essa consiste in un USER ID associato ad una PASSWORD. Lo USER ID non può essere assegnato ad altri incaricati, neppure in tempi diversi.
La password deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi. Per agevolare la corretta gestione del cambio password, è stato adottato un meccanismo di scadenza automatica della stessa.

Gestione USER ID e profilazione di accesso utenti

Sarà cura dell'Amministratore di Sistema, far sì che ogni USER ID venga attribuito in maniera da identificare univocamente l'utente e in modo che lo stesso USER ID non possa essere condiviso con altri incaricati, neppure in tempi diversi.
All'atto dell'assunzione o in caso di cambiamento degli ambiti di trattamento consentiti all'utente, la Direzione dovrà comunicare all'Amministratore di Sistema le esigenze di accesso alla rete (casella email, area di memorizzazione file ecc.) e la profilazione per l'accesso al software gestionale, nonché l'elenco delle applicazioni e delle banche dati a cui l'incaricato dovrà poter accedere per lo svolgimento delle proprie mansioni.

Gestione password

Ogni utente è responsabile del corretto uso della propria password che deve essere considerata strettamente personale e non comunicata ad altri per alcun motivo.
Inoltre una gestione poco attenta della propria password rende inefficace il meccanismo di autenticazione e potrebbe quindi consentire ad un'altra persona un accesso illecito alla rete e/o all'applicazione e di conseguenza ai dati in essi custoditi.
Se il proprietario della password, per sua volontà o scarsa attenzione, permette ad altre persone di venire in possesso della sua password, tutte le operazioni effettuate da tali persone verranno attribuite al proprietario stesso, il quale pertanto risulterà responsabile di tutti gli illeciti commessi.
Nel caso si sospetti che la password abbia perso la segretezza o in caso di dimenticanza della stessa, è necessario avvertire l'Amministratore di Sistema che metterà l'utente in grado di inserire una nuova password.

Istruzioni per la password

- deve essere composta da almeno 8 caratteri alfanumerici
- deve rispettare almeno 3 dei 4 seguenti requisiti: 1 lettera maiuscola, 1 minuscola, 1 numero, 1 carattere speciale
- non deve essere uguale a quella precedente
- non deve contenere riferimenti agevolmente riconducibili all'utente (non scegliere il proprio nome o cognome, soprannome, data di nascita, il nome di persone, parole comuni, nomi di paesi, animali e così via)

E' responsabilità dell'utente:

- Non dare la propria password ad altri
- Non lasciare la password su un biglietto tipo post-it in vista
- Non scrivere la password su un pezzo di carta e gettarla nel cestino
- Non farsi spiare quando si digita una password

Si raccomanda inoltre di:
- Non usare la stessa password per più scopi
- Non usare proverbi, nomi di personaggi famosi, titoli di film e brani musicali: alcuni sistemi avanzati utilizzati per intercettare le password li contengono nel loro dizionario interno
- Non usare parole del vocabolario
- Usare tecniche mnemoniche con frasi senza senso per ricordare la password
- Creare una password partendo da una frase, ad esempio:
    - Nel 98 ho traslocato a Modena: IO98->MO
    - mio cane pesa 12 chili: lmC=12Kg
    - Andare al mare o in montagna?: AaM!iM?

Accesso ai dati sul Sistema Informativo in caso di assenza o di cessazione del rapporto di lavoro

Qualora si rendesse necessario, per impedimento o prolungata assenza di un incaricato, accedere ai dati da questi trattati e non fosse possibile farlo attraverso un utente con profilo/ruolo ed incarico analogo, il Capo ufficio/Responsabile di riferimento ha la facoltà di richiedere all'Amministratore di Sistema di disabilitare la password dell'incaricato assente ed inserirne una provvisoria di durata temporanea.
A tal fine il Responsabile di riferimento invierà una e-mail di richiesta all'Amministratore di Sistema (e in copia conoscenza alla Direzione) al fine di resettare le credenziali del lavoratore assente.

Il Responsabile di riferimento provvederà poi a darne debita informazione all'incaricato al suo ritorno, affinché questi possa ripristinare al più presto la segretezza delle proprie credenziali.
Si ritiene comunque opportuno, ogni qualvolta possibile, contattare preventivamente l'incaricato assente e concordare con quest'ultimo le modalità di gestione della specifica esigenza (ad esempio designando e autorizzando un collega ad accedere ai dati previo reset della password e inserimento di password temporanea).

Alla cessazione del rapporto di lavoro di un lavoratore abilitato ad accedere al Sistema Informativo, il Capo Ufficio informerà l'Amministratore di Sistema (e in copia conoscenza alla Direzione) che provvederà immediatamente, a far disattivare le utenze (account di rete, casella email, user gestionale); la cancellazione effettiva dei dati dell'utente sarà effettuata al più presto a meno che il responsabile del lavoratore cessato ne richieda esplicitamente il mantenimento specificandone finalità e durata (via email all'Amministratore di Sistema, in copia alla Direzione) e comunque per un massimo di 30 giorni.
Ogni rispettivo capo ufficio dovrà assicurarsi che l'utente – prima della cessazione – provveda a rendere disponibili i propri dati, file e messaggi e-mail, memorizzati nel Sistema Informativo e a concordare per tempo con l'Amministratore di Sistema (via e-mail, in copia alla Direzione) tempistica e modalità di disattivazione dell'account di rete, casella email e utenza software gestionale.

L'utilizzo della postazione di lavoro

Il terminale, il personal computer (fisso e portatile) ed i relativi programmi e/o applicazioni affidati al lavoratore sono strumenti di lavoro.
Si fa rilevare che ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'utente è responsabile del personal computer o altro dispositivo assegnatogli dall'Azienda.

Pertanto:

- Tali strumenti vanno custoditi in modo appropriato;
- tali strumenti possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tantomeno per scopi illeciti;
- nel caso dei PC portatili questi andranno custoditi con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Agli utenti non è consentito:

- Utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- Utilizzare programmi non distribuiti approvati/licenziati ufficialmente dalla Direzione;
- Modificare le configurazioni impostate sul proprio PC;
- Utilizzare supporti di memorizzazione (hdd removibili, pen drive Usb, modem, masterizzatori, etc.) non autorizzati dal da ICT;
- Archiviare dati sui PC locali salvo autorizzazione della Direzione;
- Scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria posizione lavorativa (ad esempio file musicali);
- Installare sul proprio PC mezzi di comunicazione propri (come ad esempio i modem);
- Ascoltare, sui PC dotati di scheda audio e/o di lettore CD, programmi, file audio o musicali, se non a fini prettamente lavorativi;
- Riprodurre o duplicare programmi informatici ai sensi delle Legge n.128 del 21.05.2004;
- Eseguire sistemi operativi live da CD/DVD, chiavi USB, HD esterni/interni o tecniche di virtualizzazione, salvo autorizzazione dei tecnici aziendali preposti;
- Collegare pc portatili o altri dispositivi mobili non aziendali alla rete, salvo autorizzazione della Direzione.

Il PC deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. L'utente è tenuto ad attivare il salvaschermo del PC con password o a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un computer incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che ve ne sia la possibilità di provarne in seguito l'indebito uso.

Si ricorda infine che quanto più il desktop è occupato da icone, file o anche solo da collegamenti, tanto più lento sarà il caricamento del profilo all'avvio, ad esempio al mattino al momento dell'accensione.

Pertanto si raccomanda di mantenere pulito e ordinato il desktop del proprio computer.

Regole per le persone esterne

- Ai visitatori non è permesso connettere i propri equipaggiamenti direttamente alla rete di **Holding Ferrara Servizi Srl e/o delle sue controllate** se non previa autorizzazione della Direzione.
- Per l'accesso a Internet può essere messa a disposizione degli ospiti una rete WiFi "Guest" separata a livello logico dalla rete aziendale.
- Consulenti e altre persone esterne che operano con continuità in **Holding Ferrara Servizi Srl e/o nelle sue controllate** possono essere inclusi nella rete interna con un ID personale e una password firmando un apposito impegno.
- Consulenti che necessitano di connettersi alla rete aziendale da remoto sono accettati solo se preventivamente autorizzati da **Holding Ferrara Servizi Srl e/o dalle sue controllate** e con obbligo di utilizzare canali di accesso sicuri (es.: VPN) . La parte esterna dovrà firmare un apposito impegno.

Copyright e licenze d'uso

Solamente il software coperto da licenza d'uso può essere utilizzato nell'ambito del Sistema Informativo, pertanto, relativamente a qualsiasi software (programmi, file, immagini, testi, video, suoni, ecc.), gli utenti si impegnano a richiedere alla Direzione un'autorizzazione scritta prima di procedere a qualsiasi copia, download o installazione di qualsiasi genere

Ciascuna Direzione Aziendale provvederà a:

- redigere e mantenere aggiornato un elenco delle licenze d'uso disponibili in **Holding Ferrara Servizi Srl e nelle sue controllate**;
- verificare periodicamente (almeno una volta ogni anno) il sw installato sui computer.

Ulteriori regole in caso di utilizzo di PC portatili

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete.
Tutti i computer portatili assegnati in dotazione, sono strumenti di proprietà della **Holding Ferrara Servizi Srl o delle sue controllate** destinati ad un utilizzo professionale. L'utente si impegna quindi, sotto la propria responsabilità, ad assicurarne l'uso per scopi di lavoro; si impegna altresì a prevenirne l'uso da parte di terzi (famigliari, amici ecc.)

Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (CD, DVD, USB, dischetti, cassette, ecc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
Si ricorda infatti che quando un file viene rimosso i dati non vengono effettivamente cancellati, neanche a seguito di formattazione, a meno di non utilizzare appositi programmi software. Pertanto, nell'impossibilità di garantire la cancellazione sicura, non lasciare che terzi riutilizzino il supporto magnetico e, nel dubbio, utilizzare un supporto nuovo. I supporti magnetici contenenti dati sensibili devono essere custoditi in armadi o cassetti chiusi a chiave.

Utilizzo dei Server Aziendali

I server di rete sono aree di condivisione di informazioni strettamente professionali 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 o sui PC locali.
Holding Ferrara Servizi Srl e le sue controllate si riservano 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 manuale.
Ogni utente è tenuto a memorizzare i propri file nella/e area/e del Sistema Informativo appositamente predisposte, e non dovrà memorizzare file nel "desktop" in quanto quest'ultimo non è sottoposto alle procedure di backup.
Particolare attenzione deve essere riposta nell'archiviare documenti a carattere riservato all'interno di cartelle situate sui server e condivisibili da più utenti del medesimo servizio o da parte di più uffici; è necessario infatti evitare che tali documenti possano essere letti o addirittura modificati da persone non autorizzate.

Sui Server vengono inoltre svolte le comuni e regolari attività di controllo, amministrazione e backup da parte del personale addetto.

Prevenzione dei malware

I virus sono programmi in grado di trasmettersi in modo autonomo e possono causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.
Oggi, meglio che soltanto di virus, è più corretto parlare di *malware*, che oltre ai virus comprendono -a titolo esemplificativo e non esaustivo- i cosiddetti *trojan* (cavalli di Troia), gli *Spyware* e altri strumenti e modalità di attacco difficilmente classificabili.
I mezzi a disposizione per difendersi dai *malware* includono la protezione dagli accessi non autorizzati, il ricorso esclusivo a fonti note e sicure per dati e programmi, l'uso dei software *antimalware* aggiornati.

L'Amministratore di Sistema, provvederà a:
- far installare e mantenere aggiornato un adeguato software antimalware;
- cancellare ogni malware intercettato e documentare ogni caso che si verifichi.

E' responsabilità dell'utente:
- Evitare di introdurre consciamente un *malware* nei computer.
- Utilizzare esclusivamente i supporti di memorizzazione (CD, DVD, USB, cassette, ecc.) ricevuti in dotazione.
- Non utilizzare programmi non autorizzati o software gratuito prelevato da siti Internet o in allegato a riviste o libri.
- Qualora si fosse costretti ad utilizzare supporti di memorizzazione (v. sopra) di incerta provenienza, effettuare prima una scansione *antimalware*.
- Ogni programma deve essere sottoposto alla scansione prima di essere installato.
- Non far partire, anche in modo accidentale, il computer da supporti esterni removibili (chiavette USB, CD, DVD…).
- Non utilizzare supporti già adoperati in precedenza o preformattati.
- Non utilizzare modem per la posta elettronica.
- Non scaricare da Internet, se non previa autorizzazione, file eseguibili o documenti da siti FTP.
- Non scaricare da Internet file di cui non si conosce o non si è ragionevolmente sicuri della fonte.
- Evitare di navigare in siti non consentiti o non affidabili (vedi anche più avanti l'apposito paragrafo "L'utilizzo di Internet")
- Non aprire e-mail di cui non si è certi della fonte, né i relativi allegati, in particolare se si dovesse trattare di file eseguibili (.exe) o compressi (.zip).
- Evitare di "cliccare" sui collegamenti (link) proposti all'interno delle e-mail.
- Contattare immediatamente l'Amministratore di Sistema qualora dovesse riscontrare o sospettare la presenza di *malware* nel computer che sta utilizzando.

Gestione dei backup / Archiviazione

Dati gestiti sui server centralizzati.

I dati e i file di lavoro devono essere archiviati sui server centralizzati.
Il sistema di rete è predisposto per la copia automatizzata dei dati contenuti nei server centralizzati.
Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili o loro trasferimento su supporti ottici. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

Dati gestiti sui PC locali o portatili

Ove per l'archiviazione dei dati non siano utilizzati server centralizzati ma PC locali o portatili, sarà cura dell'incaricato stesso provvedere a trasferire appena possibile nella propria area di memorizzazione (cartella) del Sistema Informativo i dati salvati nel PC: i dati saranno così soggetti alle procedure di backup standard controllate dall'Amministratore di Sistema.

Il trasferimento dei dati nelle cartelle del server deve avvenire con frequenza commisurata alla frequenza con cui i dati sono aggiornati o, nel caso di utilizzo di PC portatili, ogni volta che l'utente rientra in sede e si collega alla rete aziendale.

INTERNET E POSTA ELETTRONICA

L'utilizzo di Internet

Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet; inoltre, attraverso la rete possono essere introdotti nel sistema virus informatici Spyware, Malware, e possono attraverso "*backdoor*" penetrare utenti non autorizzati.

Internet è da considerarsi uno strumento aziendale e pertanto l'utilizzo di Internet da parte dei lavoratori dovrà essere adeguato a scopi e obiettivi aziendali e conforme agli standard di comportamento dell'Azienda.

L'utilizzo di Internet per uso personale è consentito purché non interferisca con la normale attività lavorativa e nel rispetto delle regole e dei criteri riportati di seguito..

E' sempre vietato l'utilizzo di Internet per scopi illegali, non etici o rischiosi per l'Azienda.

Per salvaguardare la sicurezza del Sistema Informativo, è impedito, tramite l'uso di strumenti software dedicati, l'accesso ad alcune categorie di siti internet considerati potenzialmente pericolosi o incompatibili con l'etica di **Holding Ferrara Servizi Srl e delle sue controllate**.

E' sempre espressamente vietato:

- navigare in siti che possono rivelare le opinioni politiche, religiose o sindacali del lavoratore;
- accedere a siti web dal contenuto offensivo, pornografico, discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o comunque illegale in qualsiasi formato (programmi, immagini, testi, video, suoni, …)
- memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- scaricare file di grandi dimensioni ed effettuare navigazioni ad elevato consumo di banda, se non espressamente autorizzato dalla Direzione;
- scaricare software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla Direzione;

A corollario di quanto sopra, si raccomanda di non fornire a terzi notizie relative a strumenti informatici, nominativi di utenti, procedure o qualsiasi altro elemento potenzialmente utilizzabile per attacchi miranti a danneggiare il Sistema Informativo.

Documentazione dell'attività di navigazione

L'accesso ai siti internet da parte degli utenti può essere documentato automaticamente in un file di log che riporta, in forma anonima e tale da precludere l'immediata identificazione degli utenti, i dettagli della navigazione, ed elenca i siti e i documenti che gli utenti hanno consultato.
I log file sono memorizzati in modo protetto e potranno eventualmente essere visionati da:

- Legali rappresentanti dell'Azienda
- Amministratori di sistema (solo per fini legati alla sicurezza informatica).

I file di log potranno essere conservati per un periodo massimo di 30 giorni.
I file di log potranno essere messi a disposizione dell'autorità di controllo e/o giudiziaria in caso di ispezioni e/o accertamenti.

Utilizzo della posta elettronica

Si precisa che la casella di posta aziendale assegnata all'utente è uno strumento di lavoro; pertanto l'utente dovrà assicurarsi che ogni contatto sulla propria email aziendale sia dovuto a ragioni esclusivamente professionali.

E' consentito l'utilizzo delle caselle di posta personali (non aziendali) purché non interferisca con l'attività organizzativa. Nell'utilizzo della propria webmail privata attraverso internet l'utente avrà cura di evitare i rischi connessi a un utilizzo potenzialmente pericoloso quali ad esempio eseguire il download di allegati potenzialmente infetti o seguire link presenti nel testo dei messaggi.

Le persone assegnatarie delle casella di posta elettronica sono responsabili del corretto utilizzo delle stesse. In particolare queste dovranno di norma controllare la posta in arrivo almeno una volta al giorno e, se necessario, inoltrare correttamente e tempestivamente la posta in entrata non a loro direttamente indirizzata.

Ogni comunicazione diretta al dominio *"www.holdingferrara.it"* deve intendersi diretta alla **Holding Ferrara Servizi Srl**. Analoghe considerazioni sono per **le sue controllate** e i relativi domini.

Agli utenti non è consentito:

- Utilizzare la posta elettronica aziendale "*nome.cognome@holdingferrara.it"* o "*ufficio@holdingferrara.it"* per motivi non attinenti allo svolgimento delle mansioni assegnate - lo stesso vale per gli indirizzi di posta elettronica delle società controllate;
- Utilizzare la posta elettronica aziendale "*nome.cognome@holdingferrara.it"* o "*ufficio@holdingferrara.it"* per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione assegnate - lo stesso vale per gli indirizzi di posta elettronica delle società controllate;
- Spedire o far circolare catene di messaggi ("catene di Sant'Antonio" e simili);
- Spedire lo stesso messaggio di posta elettronica a un numero elevato di utenti contemporaneamente o a più di una lista di distribuzione;
- Richiedere l'invio di e-mail ad uso personale o che non riguardano le attività lavorative;
- Inviare o ricevere messaggi dal contenuto offensivo, pornografico, discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o comunque illegale in qualsiasi formato (programmi, immagini, testi, video, suoni, …);
- Diffondere opinioni personali come se fossero opinioni aziendali;
- Diffondere messaggi di provenienza dubbia;

Si ricorda che i messaggi di posta elettronica viaggiano in chiaro e sono pertanto intercettabili da chiunque con pochissima difficoltà. Si richiede quindi particolare attenzione nell'utilizzare la posta elettronica esterna per inviare documenti di lavoro "riservati" in quanto possono essere intercettati da estranei.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di grande dimensione.

Si raccomanda di fare attenzione agli allegati di posta elettronica prima del loro utilizzo, non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti e, in caso di dubbio, contattare l'Amministratore di Sistema.
Si raccomanda inoltre di includere ed aggiornare il proprio nome e posizione svolta presso la **Holding Ferrara Servizi Srl e le sue controllate** in fondo al messaggio (footer) nel caso di comunicazioni verso l'esterno.

Procedura per accedere alla posta del lavoratore assente.

Holding Ferrara Servizi Srl e le sue controllate adottano le opportune procedure al fine di garantire la continuità del servizio in caso di assenza del lavoratore.

In caso di assenza programmata (ferie, permessi,..) al lavoratore è richiesto di attivare la funzione di risposta automatica contenente l'indicazione della durata dell'assenza e di un contatto alternativo al quale rivolgersi in caso di urgenza, oppure l'inoltro automatico a un collega .

Nel caso di assenza improvvisa, non programmata o prolungata, e solo in presenza di improrogabili necessità legate all'attività lavorativa, l'interessato potrà delegare un altro lavoratore (fiduciario da designare attraverso comunicazione scritta al fiduciario medesimo e in copia alla Direzione) a verificare il contenuto di messaggi e a inoltrare al Capo Ufficio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Nel caso di mancata designazione del collega fiduciario, e sempre e comunque in presenza di improrogabili necessità legate all'attività lavorativa, il Capo Ufficio, avvalendosi dell'Amministratore di Sistema, potrà accedere alle e-mail e verificare il contenuto di messaggi indirizzati al lavoratore assente.

Al rientro del lavoratore dopo l'assenza il Capo Ufficio dovrà informarlo per iscritto, motivandolo, dell'avvenuto accesso alla sua casella di posta.

ALTRI BENI AZIENDALI

Telefoni aziendali fissi

I telefoni aziendali sono uno strumento di lavoro dato in dotazione dall'Azienda ai lavoratori per l'espletamento delle loro mansioni. Il loro utilizzo è consentito anche per uso personale purché questo non interferisca con l'attività lavorativa.

Se si hanno a disposizione dei telefoni con dispositivo 'Viva Voce', ci si deve sincerare che l'ascolto della conversazione sia effettuato con la porta chiusa evitando che persone non interessate alla conversazione possano ascoltare.

Fax aziendali

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte della Direzione.

Telefoni cellulari

I telefoni cellulari (compresi smartphone e altri dispositivi di telefonia mobile) sono assegnati in dotazione per l'uso lavorativo. Il loro utilizzo è consentito anche per uso personale purché questo non interferisca con l'attività lavorativa e nel rispetto dei criteri riportati di seguito.

In generale, i telefoni non possono essere ceduti né fatti utilizzare a terzi (famigliari, amici ecc.), eccetto colleghi, collaboratori, consulenti o soggetti autorizzati.
In particolare, in modo non esaustivo, vengono posti i seguenti divieti:

- Non è consentito modificare le caratteristiche hardware e software impostate sul telefono.
- Non è consentita l'installazione di programmi (App) diversi da quelli autorizzati.
- Non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
- Non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione.
- Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al telefono, se non quelli aziendali o quelli autorizzati.

Dati di traffico e tabulati telefonici

Si ricorda che i numeri chiamati possono essere tracciati e riportati in tabulati, utilizzati di norma a fini statistici e di contenimento costi.

CONTROLLI E VIOLAZIONI

L'Azienda, ai fini di sicurezza o per motivi tecnici e per la propria tutela, si riserva di effettuare controlli, saltuari ed occasionali, nei limiti consentiti dalle norme vigenti e nelle modalità previste dal citato provvedimento del Garante.

Detti controlli vengono eseguiti in modo preliminare su dati aggregati e comunque anonimi, nel pieno rispetto dei principi di pertinenza e non eccedenza e, salvo impossibilità dettata dall'urgenza, conclusi da avvisi generalizzati.
Perdurando le condizioni di anomalia, saranno a questo punto giustificati controlli su base individuale.

Nei casi di accertata violazione delle disposizioni contenute nel presente regolamento, è demandata alla Direzione che ha la competenza del servizio l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituenti reato.

La responsabilità, anche penale, specificatamente prevista dal D.Lgs. 196 del 30 giugno 2003 per un eventuale uso dei dati personali conosciuti non conforme alle indicazioni impartite dal titolare o dal responsabile, resta a carico della singola persona cui l'uso illegittimo sia imputabile.

In caso di sanzioni di natura pecuniaria o richieste di risarcimento danni, l'Azienda ha la facoltà di rivalersi sull'autore materiale dell'illecito.