TRENTINO DIGITALE S.P.A.

Regolamento corretto utilizzo risorse aziendali - Terze parti

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
07/10/2011	01.00 Obsoleta	Prima emissione
14/06/2012	01.01 Obsoleta	Sostituzione del riferimento SIC-POL-06 (soppressa) con SIC-STD-19
19/09/2019	02.00 In vigore	Aggiornamento template e contenuto del documento
16/10/2020	02.1 In vigore	Modifica regole per la posta elettronica.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

Regolamento Corretto Utilizzo Risorse Aziendali - Terze Parti

INDICE

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

1 Introduzione

1.1 Premessa

La sicurezza delle informazioni è strettamente dipendente dal rispetto di alcune regole di comportamento concernenti:

- la tutela dei luoghi di lavoro e delle risorse aziendali utilizzate nell'ambito dell'attività lavorativa;
- il corretto utilizzo delle risorse attraverso le quali vengono gestiti dati ed informazioni.

Lo scopo del presente documento è quello di definire un insieme di norme comportamentali di buona condotta cui tutte le terze parti che operano per Trentino Digitale devono uniformarsi, per garantire le esigenze di protezione delle informazioni.

Le norme comportamentali in materia di sicurezza aziendale, descritte nel seguito, sono state strutturate in modo da recepire anche alcune delle richieste provenienti dal codice in materia di protezione dei dati personali (D.Lgs. 196/2003).

1.2 Perimetro organizzativo

La presente policy si applica a tutto il personale non dipendente – terze parti – che opera per Trentino Digitale ossia:

- collaboratori esterni fuori sede: soggetti che collaborano con Trentino Digitale da remoto e che accedono alle risorse aziendali attraverso connessioni VPN;
- collaboratori esterni in sede: soggetti che collaborano con Trentino Digitale presso la sede della società stessa esclusivamente per periodi limitati (anche questa categoria di soggetti accede alle risorse aziendali attraverso connessioni VPN);
- utenti nomadici: soggetti che hanno necessità di accedere solo ad Internet per brevi periodi di tempo e che operano presso la sede della società (es. consulenti, docenti).

Come definito nella lettera di arrivo firmata dalle terze parti e nel contratto con l'azienda di appartenenza, il mancato rispetto delle norme riportate nel presente documento, consultabile presso la funzione Sicurezza, costituisce inadempimento contrattuale (fatte salve le ulteriori ed eventuali responsabilità civili e penali).

1.3 Termini e definizioni

Backup - Salvataggio/copia di sicurezza, raccolta di dati ed informazioni su un supporto diverso da quello usato normalmente al fine di garantire il recupero delle informazioni in caso di danneggiamento del supporto primario.

Denial of Service – Attività malevola volta a bloccare la normale operatività di un host, o di un suo servizio.

e-mail bomb – Messaggio di posta elettronica inviato per impedire il regolare funzionamento del mail server destinatario.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

Regolamento Corretto Utilizzo Risorse Aziendali - Terze Parti

Malware – E' un qualunque software creato con lo scopo di causare danni sul computer su cui viene attivato e/o eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* che in italiano è equivalente a "*codice maligno*".

Ping flood - Invio di un elevato traffico di rete verso un determinato host con lo scopo di bloccare qualunque suo tentativo di comunicazione verso l'esterno.

Port scanning - Interrogazione massiva di tutte le porte TCP/IP di un determinato host con lo scopo di individuare quelle attive.

Security scanning – Attività di analisi, mediante appositi software, per individuare le eventuali debolezze di security presenti su un determinato host.

Sniffing - Attività di intercettazione dei dati che vengono trasmessi su una rete.

Spam - Invio non autorizzato e/o non richiesto di posta elettronica.

Spoofing – E' un tipo di attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità (spoof).

Terze parti – Soggetti esterni che collaborano con Trentino Digitale (utenti nomadici, collaboratori esterni).

Utente nomadico – Utente esterno che deve accedere ad Internet per brevi periodi temporali (es. consulenti, docenti).

Virus – Software che ha il solo scopo di replicarsi e danneggiare i sistemi che lo ospitano.

VPN (Virtual Private Network) – Una Virtual Private Network o VPN è una rete privata virtuale instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come Internet. Lo scopo delle reti VPN è di garantire un livello di sicurezza pari, o superiore, ad una connessione dedicata utilizzando reti pubbliche condivise.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

1.4 Riferimenti

Norme di legge	*Regolamento (UE) 2016/679 "Regolamento generale sulla protezione dei dati"* *D.lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss. mm. ii.* Del. n. 13 del 01/03/2007 - *Lavoro: le linee guida del Garante per posta elettronica e internet* D.Lgs. 231/2001- *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*
Standard di Riferimento	-
A documenti del Sistema Sicurezza	SIC-STD-19 *"Accesso alla rete di Trentino Digitale"* SIC-IO-01 *"Modalità di accesso ai dati degli incaricati"* SIC-IO-03 *"Gestione delle richieste di categorizzazione della piattaforma di URL filtering"* SIC-IO-10 *"Modalità richieste accesso logico"* SIC-STD-08 *"Norme per la raccolta e la conservazione dei dati relativi al traffico di rete"* SIC-STD-07 *"Elenco siti inibiti alla navigazione"*
A documenti del Sistema di Gestione della Qualità	-
Altri documenti aziendali	231-CE – *"Codice etico e di comportamento interno"*

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

2 Norme

2.1 Principi Generali

L'obiettivo del presente regolamento è di favorire il contenimento dei rischi ad un livello accettabile mediante un insieme di misure di protezione organizzative, operative e tecnologiche finalizzate a:

- preservare il patrimonio informativo aziendale;
- garantire la fiducia e la soddisfazione della clientela, tutelando e proteggendo i dati di loro titolarità o relativi ai servizi loro erogati;
- garantire la riservatezza ed integrità delle informazioni;
- garantire la continuità del servizio;
- adempiere a quanto espressamente disposto dalla normativa italiana in materia di sicurezza dei dati, con particolare riferimento al codice in materia di protezione dei dati personali (D.Lgs.196/03);
- dotare la società di un modello organizzativo, di gestione e controllo conforme alle previsioni di legge (D.Lgs. 231/2001).

Quanto riportato nel presente documento recepisce ed integra quanto descritto nel codice etico aziendale 231-CE *Codice etico e di comportamento interno*.

Le misure di sicurezza adottate rispondono anche a precisi obblighi di legge la cui attuazione potrà conseguentemente essere oggetto di verifiche mirate. Trentino Digitale non effettua verifiche preventive sull'utilizzo degli strumenti informatici e dei servizi messi a disposizione dei propri collaboratori; la società si riserva tuttavia la facoltà di effettuare generici controlli sull'osservanza di quanto stabilito all'interno del presente regolamento e di procedere con indagini più puntuali in presenza di comportamenti anomali.

Inoltre, l'integrità e il diritto di uso esclusivo dei dati, programmi e in generale sistemi informativi della società risultano espressamente tutelati da specifiche norme di legge la cui violazione comporta l'adozione di sanzioni anche di carattere penale.

Ciò premesso, tutti i collaboratori esterni sono tenuti alla scrupolosa osservanza delle disposizioni finalizzate a garantire e tutelare il patrimonio informativo e ad adottare comportamenti conformi a quanto stabilito nel presente regolamento.

Il mancato rispetto delle norme definite all'interno del presente regolamento costituisce inadempimento contrattuale (fatte salve le ulteriori ed eventuali responsabilità civili e penali).

2.2 Gestione dei locali e delle risorse fisiche

I locali e tutte le risorse fisiche fornite da Trentino Digitale devono essere utilizzate e custodite con la massima diligenza al fine di garantire un'efficiente conduzione dell'attività lavorativa e un adeguato livello di sicurezza delle informazioni.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

Nei paragrafi successivi sono descritti i comportamenti a cui tutti i collaboratori esterni, che hanno accesso ai locali e alle risorse fisiche di Trentino Digitale, devono attenersi per garantire la sicurezza fisica di aree ed asset aziendali.

2.2.1 Gestione dei locali

Con il termine "*Gestione dei locali*" viene di seguito fatto riferimento all'insieme di comportamenti cui è necessario attenersi per garantire la sicurezza delle informazioni contenute nelle aree e negli uffici di Trentino Digitale.

In particolare l'azienda ritiene che tutte le terze parti che operano presso i propri locali debbano rispettare le seguenti norme:

- l'accesso allo stabile, alle aree protette, alle aree ristrette e agli archivi è regolamentato da specifiche istruzioni aziendali cui occorre attenersi: solo le persone che hanno precise e motivate esigenze di accedere a tali ambienti, per finalità lavorative, possono detenere la relativa chiave d'accesso (o badge), che viene consegnata sulla base delle procedure vigenti in azienda;
- l'accesso alle aree protette e a quelle ad accesso ristretto deve avvenire solo in presenza di personale dipendente autorizzato;
- è vietato l'utilizzo di strumenti in grado di effettuare foto/riprese video/audio, a meno che non sia stato preventivamente autorizzato dal dirigente di riferimento.

2.2.2 Postazioni di Lavoro di proprietà delle terze parti

Gli apparati di proprietà delle terze parti e dalle stesse utilizzate, una volta connessi in VPN, rappresentano, de facto, un'estensione della rete aziendale e come tali devono essere soggetti alle stesse norme e procedure in vigore per le postazioni di lavoro gestite da Trentino Digitale.

In particolare:

- l'utilizzo della postazione di lavoro da parte degli utenti, e conseguentemente l'accesso a dati, programmi e risorse informatiche, è consentito nei limiti degli incarichi assegnati;
- tutti i PC devono essere bloccati manualmente se lasciati incustoditi e devono inoltre essere dotati di uno screen saver, protetto da password, ad attivazione automatica al massimo dopo 10 minuti di inattività;
- tutte le postazioni di lavoro devono essere dotate di software antivirus.

2.2.3 Gestione delle credenziali di accesso e della password

Qualora alle terze parti siano concessi i diritti per accedere ai sistemi informatici aziendali, tali soggetti devono essere preventivamente identificati ed autenticati, attraverso la verifica delle proprie credenziali. Qualunque variazione alle abilitazioni all'accesso alle applicazioni/archivi e/o risorse dei sistemi dovrà essere richiesta dal referente aziendale tramite l'applicativo deputato alla gestione degli accessi logici così come descritto nella SIC-IO-10 *"Modalità richieste accesso logico"*.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

Regolamento Corretto Utilizzo Risorse Aziendali - Terze Parti

Le terze parti devono prestare la massima attenzione nell'utilizzo, nella gestione e nella conservazione delle credenziali di autenticazione relative ai sistemi di Trentino Digitale. In particolare occorre:

- evitare di annotarla, in particolare all'interno dell'ufficio, o di conservarla on-line;
- evitare di rivelare la sorgente della password (es. "il mio cognome");
- evitare di comunicarla su questionari e/o moduli;
- nel caso qualcuno insista nel cercare di conoscere la password contattare il proprio referente interno che provvederà ad informare la struttura responsabile della gestione della sicurezza delle informazioni;
- fare attenzione a non digitarla nel momento in cui ci sono altre persone, nei pressi della postazione di lavoro, che potrebbero osservare tale operazione;
- evitare di utilizzare password già utilizzate in passato o utilizzate per altri scopi (es. altri servizi internet, siti web personali);
- evitare di utilizzare l'opzione "ricorda password" presente in alcuni programmi;
- in caso di dimenticanza e/o ripristino della parola chiave dovrà essere inoltrata una richiesta tramite l'applicativo deputato alla gestione degli accessi logico così come descritto nella SIC-IO-10 *"Modalità richieste accesso logico"*.

2.2.4 Gestione del software antivirus sulle postazioni di lavoro di proprietà delle terze parti

Gli apparati di proprietà delle terze parti, utilizzati dai collaboratori esterni, rappresentano de facto un'estensione della rete di Trentino Digitale e come tali devono essere soggetti alle stesse norme e procedure in vigore per le postazioni di lavoro/apparati gestiti direttamente da Trentino Digitale.

In particolare i collaboratori esterni devono:

- verificare che sia installato un software antivirus sulla propria postazione;
- accertarsi che il sistema antivirus presente sulla propria postazione di lavoro risulti sempre aggiornato (aggiornamento giornaliero);
- evitare di disabilitare, per qualsiasi motivo, il sistema antivirus;
- verificare, prima di aprirli, attraverso l'utilizzo dell'antivirus tutti i programmi / documenti ricevuti, via mail o mediante supporto hardware, o scaricati da Internet.

2.3 Principi per la gestione sicura dei servizi aziendali

2.3.1 Premessa

Trentino Digitale, per permettere il regolare svolgimento dell'attività lavorativa, mette a disposizione di alcuni collaboratori esterni dei servizi quali la posta elettronica e la connessione a Internet.

Tali servizi rappresentano degli strumenti aziendali messi a disposizione delle terze parti esclusivamente per finalità di natura lavorativa; è facoltà della società decidere, a suo insindacabile giudizio, a quali soggetti concedere tali strumenti. Trentino Digitale è infatti esclusiva titolare e proprietaria/licenziataria degli strumenti informatici, che vengono messi a disposizione degli utenti ai soli fini dell'esecuzione dell'attività lavorativa e professionale. Ugualmente, Trentino Digitale è titolare e proprietaria di tutte le

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

informazioni, le registrazioni ed i dati che sono contenuti e/o trattati mediante i suddetti strumenti informatici.

Di seguito sono riportate le norme, per quanto concerne le modalità di utilizzo, alle quali dovranno attenersi le terze parti qualora risultino dotate di una casella di posta aziendale e/o di una connessione alla rete Internet. Vengono inoltre descritti i criteri adottati per il controllo delle stesse.

2.3.2 Regole per l'utilizzo della rete aziendale

I collaboratori esterni autorizzati ad accedere alla rete intranet di Trentino Digitale (per dettagli fare riferimento a SIC-STD-19 *"Accesso alla rete di Trentino Digitale"*) devono accedere alla rete sempre tramite connessioni VPN (sia che lavorino direttamente dalla sede di Trentino Digitale sia che lavorino da remoto) e hanno la responsabilità di garantire, alla connessione via VPN, la stessa attenzione e diligenza applicata ad una connessione diretta.

2.3.3 Regole per la navigazione in Internet

L'accesso ad Internet alle terze parti è fornito allo scopo di consentire l'acceso ad eventuali informazioni necessarie allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro, i soggetti cui la società attribuisce l'accesso sono responsabili del suo corretto utilizzo. In particolare, si devono osservare le seguenti regole:

- è vietata la navigazione su siti contrari all'etica, al buon costume o aventi contenuti illegali;
- è vietata la condivisione di file in modalità peer-to-peer;
- è vietato scaricare programmi, anche se privi di licenza o in prova (freeware e shareware), se non in caso di espressa autorizzazione da parte del proprio referente o della struttura responsabile della gestione della sicurezza delle informazioni; eseguire il download di file da Internet è, infatti, un'operazione intrinsecamente pericolosa in quanto può essere il veicolo per l'introduzione di virus e malware;
- rispettare i diritti d'autore, che siano essi appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale compreso, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietato immettere sulla rete o sui server software dannoso per i sistemi o comunque non autorizzato;
- è vietato utilizzare l'infrastruttura tecnologica dell'azienda per procurarsi e diffondere materiale in violazione con le normative vigenti;
- è vietato generare dei problemi di sicurezza o danneggiare le comunicazioni sulla rete. I problemi di sicurezza includono, ma non sono limitati a, accedere a dati e/o server per i quali non si è specificatamente autorizzati, effettuare ping flood o spoofing di pacchetti;

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'utente;
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account;
- le attività di Port Scanning o Security Scanning sono espressamente proibite a meno che non vengano notificate e autorizzate dalla struttura responsabile della gestione della sicurezza delle informazioni;
- è vietato interferire o bloccare l'operatività di qualunque utente (es. Denial of Service Attack);
- è vietato utilizzare qualunque programma/script/comando o spedire messaggio di qualunque tipo, sia localmente che via Internet/Intranet/Extranet, con l'intento di interferire o disabilitare una qualunque connessione di altri utenti;
- è proibito creare, trasmettere, pubblicare e/o archiviare qualsiasi tipo di materiale:
    - che infranga le leggi sul diritto d'autore e la proprietà intellettuale;
    - che includa contenuti che siano dannosi, minatori, molesti, offensivi, calunniosi o volgari;
    - che violi le leggi sulla Privacy;
    - che incoraggi il compiersi di azioni criminali e che, in generale, possa arrecare danno all'azienda;

le richieste di accesso a siti Internet, provenienti da utenti connessi alla rete di Trentino Digitale, devono essere verificate e autorizzate dall'infrastruttura di Url filtering: è facoltà dei direttori e dei dirigenti di riferimento richiedere, tramite l'applicazione di accesso logico, ulteriori restrizioni o particolari concessioni (rif. SIC-IO-03 *"Gestione delle richieste di categorizzazione della piattaforma di URL filtering"*). In particolare, in ottemperanza con quanto previsto anche dalla Del. n. 13 del 1° marzo 2007, la società ha individuato le categorie di siti considerati non correlati con la prestazione lavorativa, quale misura volta alla tutela ed alla prevenzione di un utilizzo improprio di Internet. Viene quindi bloccata la navigazione verso i soli siti che rientrano nelle macro categorie identificate all'interno del documento SIC-STD-07 *"Elenco siti inibiti alla navigazione"*.

2.3.4 Regole per l'utilizzo della Posta Elettronica fornita da Trentino Digitale

Trentino Digitale mette a disposizione di alcuni collaboratori esterni una casella di Posta Elettronica.

La casella di Posta Elettronica assegnata da Trentino Digitale all'utente ed il relativo indirizzo, nonché i messaggi in entrata ed in uscita dalla stessa, sono di proprietà aziendale. Essi rappresentano uno strumento di lavoro affidato all'utente al solo fine di consentirgli di svolgere l'incarico affidato. Le persone assegnatarie delle caselle di posta elettronica sono pertanto responsabili del corretto utilizzo delle stesse. Devono essere mantenuti comportamenti corretti nell'ambito dell'utilizzo dello strumento di posta elettronica. In particolare, valgono le seguenti considerazioni e le seguenti disposizioni:

- le caselle di posta elettronica aziendale non devono essere utilizzate per l'invio o la ricezione di messaggi personali che esulino dalle finalità lavorative o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione del referente interno. Nell'eventualità in

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

cui l'uso personale della posta elettronica aziendale si rendesse eccezionalmente necessario, gli utenti dovranno cancellare i messaggi di natura personale dal sistema non appena trasmessi e/o letti. I messaggi di posta elettronica contenuti nella casella di posta di un utente saranno infatti considerati come attinenti allo svolgimento dell'attività lavorativa dallo stesso svolta a favore della società;

- non divulgare a terzi informazioni riservate, confidenziali o comunque di proprietà di Trentino Digitale, senza espressa autorizzazione della Società stessa;
- non inviare né conservare messaggi di posta elettronica o più in generale dati, programmi o altro materiale di natura informatica dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;
- tutta la posta entrante è controllata da un software antivirus e una eventuale email infetta viene segnalata al mittente. E' comunque necessario prestare la massima attenzione nell'apertura degli allegati alle mail ricevute, indipendentemente dal fatto che si conosca o meno il mittente. In particolare non devono essere aperti documenti con nomi "anomali", né devono essere aperti file o macro ricevuti in allegato a e-mail provenienti da un mittente sconosciuto o sospetto (in questo caso segnalare immediatamente l'accaduto alla struttura competente per la gestione della sicurezza delle informazioni);
- si deve disattivare, di preferenza, la visualizzazione di messaggi di posta in formato html o, se non è possibile, adottare la massima cautela nella visualizzazione;
- non ci si deve connettere a siti web utilizzando link contenuti in e-mail provenienti da un mittente sconosciuto o sospetto, ma bisogna segnalare immediatamente l'accaduto alla struttura competente per la gestione della sicurezza delle informazioni;
- tutta la posta entrante è controllata da un software antispam: è comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale;
- gli allegati alle e-mail inviate devono avere una dimensione contenuta in modo da non rendere difficoltosa l'attività del mail server aziendale. Inoltre in particolari periodi dell'anno si vieta il massivo invio di immagini di auguri in allegato alle e-mail (es. periodo natalizio, pasquale);
- si deve disattivare l'esecuzione automatica di programmi (es. activeX) allegati ai messaggi di posta elettronica;
- inviare messaggi di posta elettronica non desiderati o richiesti, inclusa la spedizione di qualunque informazione pubblicitaria a soggetti che non abbiano specificatamente richiesto tali informazioni (spam), rappresenta una palese violazione alle norme dettate dalla legge sulla privacy. Nel rispetto della predetta norma e di quanto ad essa riconducibile è espressamente proibito alle terze parti di utilizzare i mezzi aziendali per:
    - qualunque forma di molestia via email, sia attraverso il contenuto che la frequenza di invio o le dimensioni del messaggio;
    - l'utilizzo non autorizzato dell'intestazione delle email o la creazione di intestazioni false;
    - la creazione o l'inoltro di email appartenenti a catene o similari.
- in caso di assenza prolungata e non programmata dell'utente, l'Azienda deve prevedere delle opportune procedure in grado di garantire la continuità delle attività.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

In merito a questo ultimo punto Trentino Digitale, a garanzia della continuità operativa dell'attività e della disponibilità dei dati nel caso di una eventuale assenza dell'utente (es. per ferie, malattia o attività di lavoro fuori sede) ha predisposto delle specifiche funzionalità di sistema/procedure. In particolare:

- è previsto l'utilizzo di caselle di posta di STRUTTURA, opportunamente condivise e protette, le quali sono accessibili a più di un soggetto per le comunicazioni di lavoro che possono necessitare di una consultazione da parte di più utenti.

2.3.5 Regole per l'utilizzo della Posta Elettronica non fornita da Trentino Digitale

Per l'utilizzo della posta elettronica di terzi all'interno di Trentino Digitale, devono essere rispettate le seguenti norme:

- usare cautela estrema ed evitare di aprire file allegati ad email ricevute da mittenti sconosciuti in quanto potrebbero contenere virus, e-mail bombs o altri tipi di software pericoloso per i sistemi informatici,
- evitare di visitare siti indicati in messaggi di posta elettronica ricevuti senza averli sollecitati;
- diffidare di messaggi, anche se provenienti da persone conosciute, scritti anche in lingua straniera o che chiedono di eseguire programmi (fare clic su qualche cosa, o semplicemente il passaggio del mouse);
- disattivare, di preferenza, la visualizzazione di messaggi di posta in formato html o, se non è possibile, adottare la massima cautela nella visualizzazione;
- disattivare l'esecuzione automatica di programmi (es. activeX) allegati ai messaggi di posta elettronica;
- adottare precauzioni per garantire la riservatezza dei messaggi di posta elettronica.

2.3.6 Controlli sull'utilizzo della casella di posta elettronica aziendale e del collegamento ad internet

La società, in qualità di sola ed esclusiva titolare degli strumenti informatici, nonché delle informazioni, registrazioni e dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare in ogni momento, e comunque nel rispetto dei principi di pertinenza e non eccedenza, i controlli che ritenga opportuni e necessari per le seguenti legittime finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici;
- evitare la commissione di illeciti;
- vigilare sul corretto utilizzo degli strumenti informatici (inclusa la navigazione Internet e l'uso della posta elettronica, come disciplinati nel presente regolamento) da parte degli utenti;
- verificare la funzionalità del sistema e degli strumenti informatici;
- rispondere alle richieste delle autorità giudiziarie.

Nell'effettuare i controlli per le finalità sopra specificate, la società garantisce l'assenza di interferenze o violazioni ingiustificate dei diritti e delle libertà fondamentali dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con i preventivi accorgimenti tecnici adottati da Trentino Digitale (es. filtri, configurazioni di sistemi etc.) la società si riserva la facoltà di adottare eventuali misure che consentano la verifica di comportamenti anomali attuati attraverso gli strumenti informatici.

Gli eventuali controlli saranno effettuati secondo quanto previsto nel documento "*SIC-IO-01 Modalità di accesso ai dati degli incaricati*".

Trentino Digitale garantisce comunque l'esclusione di controlli prolungati, costanti o indiscriminati, coerentemente con quanto previsto dal Provvedimento Generale del Garante della Privacy del 1 marzo 2007. Il Responsabile dei controlli, eseguiti solamente per le finalità dichiarate, è la struttura responsabile della gestione della sicurezza delle informazioni.

2.3.6.1 Controllo sul rispetto delle modalità di utilizzo della rete ed Internet

Trentino Digitale è libera di effettuare generici controlli sull'osservanza delle policy aziendali. In particolare:

- i log relativi al traffico di navigazione Internet (ora e data, ip del client, ip di destinazione e protocollo) sono salvati in appositi file in ottemperanza a quanto disposto dal Provvedimento del Garante della Privacy "*Sicurezza dei dati di traffico telefonico e telematico*" del 17 gennaio 2008;
- nei file di log non viene memorizzata nessuna informazione che permetta l'identificazione immediata dell'utente;
- tali log possono essere consultati esclusivamente per motivi di sicurezza interna o su richiesta dell'autorità giudiziaria. In nessun modo possono essere utilizzati per effettuare la profilazione delle abitudini di traffico degli utenti;
- per i dettagli in merito alle modalità di trattamento e gestione dei log fare riferimento al documento SIC-STD-08 *"Norme per la raccolta e la conservazione dei dati relativi al traffico di rete"*.

2.3.6.2 Controllo sul rispetto delle modalità di utilizzo della posta elettronica

Trentino Digitale accederà alle caselle di posta elettronica affidate agli utilizzatori nel rispetto dei limiti stabiliti nel presente documento. La società applica le seguenti modalità di gestione e controllo delle caselle di posta elettronica aziendali:

- le caselle di posta sono soggette ad attività di salvataggio (back-up) automatico, a carico del fornitore del servizio, che permette di non perdere le informazioni memorizzate anche in caso di incidenti;
- le informazioni relative ai messaggi in entrata ed in uscita dagli indirizzi di posta elettronica aziendale ed i relativi dettagli tecnici (Mittente, Data e ora di invio, Destinatario) vengono registrate e memorizzate a cura del fornitore del servizio che le fornisce in caso di richiesta formale;

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.

dal momento della cessazione della collaborazione, e solo in caso di necessità, il referente interno della risorsa può fare richiesta di accesso alla copia della casella di posta elettronica.

DOCUMENTO ED INFORMAZIONI PER CIRCOLAZIONE ED USO ESCLUSIVAMENTE INTERNI
© Tutti i diritti riservati. Proprietà Trentino Digitale S.p.A.