CRITERI E MODALITÀ OPERATIVE PER L'ACCESSO E L'UTILIZZO IN SICUREZZA DELLA RETE INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEI DIPENDENTI.

OGGETTO

Il presente disciplinare, adottato sulla base e secondo le indicazioni contenute nella deliberazione 01.03.2007 n. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica e internet", ha per oggetto i criteri e le modalità operative di accesso e utilizzo della rete internet e dei servizi su di essa accessibili da parte dei dipendenti del Comune di Trento e di tutti gli altri soggetti che a vario titolo operano nelle strutture del Comune di Trento (lavoratori socialmente utili, collaboratori, tirocinanti/stagisti).

DEFINIZIONI

Nel seguito si esplicita il significato dei termini particolari usati nel documento:

- **UTENTE INTERNET**: persona autorizzata ad accedere alla rete internet, con l'esclusione di un insieme di siti (BLACK LIST);
- **UTENTE DI POSTA ELETTRONICA**: persona autorizzata ad accedere al servizio di posta elettronica.
- **BLACK LIST**: elenco di siti non accessibili da nessun utente, perché ritenuti problematici per l'integrità dell'infrastruttura informatica o non pertinenti all'attività lavorativa.
- **INTERNET PROVIDER**: azienda che fornisce al Comune di Trento il canale di accesso alla rete internet;
- **POSTAZIONE DI LAVORO**: Dispositivo informatico collegato alla rete aziendale e abilitato ad accedere alla rete internet tramite il quale il dipendente presta l'attività lavorativa.
- **LOG**: archivio delle attività di consultazione in rete;
- **REFERENTE INFORMATICO**: soggetto che garantisce presso le singole strutture supporto al Servizio Innovazione, ricerca e transizione digitale sugli aspetti tecnici relativi ai servizi digitali;
- **DESIGNATO AL TRATTAMENTO**: soggetto designato dal titolare al trattamento di dati personali ex art. 2 quaterdecies del decreto legislativo 196/2003, individuato, per quanto previsto dal presente disciplinare, nel Dirigente del Servizio Innovazione, ricerca e transizione digitale.

MODALITÀ DI ACCESSO E DI UTILIZZO

La configurazione dei servizi di accesso ad internet e di posta elettronica viene eseguita esclusivamente dai tecnici del Servizio Innovazione, Ricerca e Transizione Digitale.

Per accedere ai servizi informatici aziendali da una postazione di lavoro l'utente dovrà utilizzare un codice identificativo (nome utente) e una parola chiave segreta (password). Se l'accesso avviene da un dispositivo esterno alla rete aziendale potranno essere necessarie

ulteriori credenziali per elevare il livello di sicurezza.

In particolare, le postazioni di lavoro fisse collegate direttamente alla rete interna comunale possono essere raggiunte anche tramite dispositivi ulteriori (di proprietà del lavoratore o forniti dall'amministrazione) e collegati alla sola rete internet. In tal caso il lavoratore utilizzerà un browser internet di ultima generazione collegandosi al servizio indicato dal Servizio Innovazione, ricerca e transizione digitale (attualmente "Guacamole"). La credenziale aggiuntiva ad utente e password per elevare il livello di sicurezza è in tal caso un codice monouso generato su base temporale (TOTP).

Le postazioni di lavoro mobili di proprietà dell'amministrazione si possono collegare alla rete aziendale tramite il servizio di Rete Privata Virtuale (VPN) dell'amministrazione. La credenziale aggiuntiva è in questo caso un certificato TLS appositamente predisposto e specifico per ogni utente.

Superato il sistema di identificazione l'utente sarà collegato alla rete aziendale e ad internet senza ulteriori formalità.

La conoscenza di nome utente e password e di eventuali altre credenziali da parte di terzi consente a questi ultimi l'accesso alla rete aziendale, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato. Le conseguenze possono essere ad esempio la visualizzazione di informazioni riservate, la distruzione o la modifica di dati, l'utilizzo indebito della casella di posta elettronica personale e di altri servizi. Pertanto l'utente si impegna a:

- non cedere, una volta superata la fase di identificazione, l'uso della propria postazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet ed agli altri strumenti di lavoro messi a disposizione dall'amministrazione comunale;
- non lasciare incustodita ed accessibile la propria postazione una volta connessi al sistema con le proprie credenziali;
- conservare le credenziali di accesso nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali di altri utenti, nemmeno se fornite volontariamente o di cui si è venuti casualmente a conoscenza;
- mantenere la corretta configurazione dei dispositivi assegnati non alterando le componenti hardware e software predisposte allo scopo, né installando ulteriore software non autorizzato;
- non salvare file audio, video e file di qualsiasi tipo non attinenti alla propria attività lavorativa negli spazi di lavoro condiviso (ad esempio unità disco diverse dal D o spazi cloud);
- rispettare le istruzioni del Servizio Innovazione, ricerca e transizione digitale e le direttive privacy, messe a disposizione sul sito intranet, nella gestione dei documenti e dati utilizzati/gestiti per l'attività lavorativa al fine di garantire adeguata protezione sia dei dati che della sicurezza del sistema.

Per prevenire la manomissione della configurazione hardware e software delle postazioni di lavoro, salvo rari casi necessari per il funzionamento di specifici applicativi, agli utenti sono assegnati diritti limitati (inferiori a quelli di amministrazione). Per l'installazione di software o la modifica della configurazioni è necessario l'intervento del referente informatico o di personale del Servizio Innovazione, ricerca e transizione digitale.

Qualsiasi azione svolta utilizzando le credenziali identificative sarà assegnata in termini di

responsabilità all'utente assegnatario delle credenziali.

L'utente sarà civilmente responsabile di qualsiasi danno arrecato alla Amministrazione e all'internet provider e/o a terzi in dipendenza della mancata osservazione di quanto previsto dal presente disciplinare.

Inoltre potrà essere chiamato a rispondere civilmente, oltre che per i propri atti illeciti, anche per quelli commessi da chiunque utilizzi le sue credenziali, con particolare riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume così come definiti dalla giurisprudenza della corte di cassazione.

La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo Provinciale di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

INTERNET

Tutti gli utenti cui è assegnata dall'Amministrazione una postazione di lavoro possono utilizzare internet, con l'esclusione di un insieme di siti (BLACK LIST), e previa identificazione con le credenziali descritte in precedenza.

La lista dei siti bloccati (BLACK LIST) utilizzata dal sistema automatico di controllo della navigazione, viene aggiornata nel tempo a cura del Servizio Innovazione, ricerca e transizione digitale anche su segnalazione dei responsabili delle strutture. La lista comprende sia siti riconosciuti come problematici per la sicurezza che siti sicuramente non pertinenti all'attività lavorativa.

Tale classificazione, non può per sua natura essere né definitiva né esente da errori; inoltre in alcuni casi può essere necessario prevedere eccezioni anche solo temporanee; le modalità di modifica della lista o l'inserimento di eccezioni temporanee vengono concordate dal Dirigente del Servizio Innovazione, ricerca e transizione digitale con il Direttore generale.

L'utente è direttamente e totalmente responsabile del proprio uso del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

All'utente non è consentito:

- servirsi o dar modo ad altri di servirsi della postazione di lavoro per l'accesso a internet legato ad attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste al Servizio Innovazione, ricerca e transizione digitale che, dopo aver verificato il rispetto delle condizioni di licenza e di sicurezza, provvederà a eseguire fisicamente lo scarico in modalità sicura ed installare il software al richiedente;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

POSTA ELETTRONICA

Il servizio di posta elettronica è da utilizzare per ragioni di servizio dagli utenti identificati con le modalità precedentemente illustrate, ai quali l'amministrazione assegna una casella di posta personale e nominativa. Eventuali comunicazioni diverse da quelle di servizio possono ritenersi ammesse, in via eccezionale e non sistematica, esclusivamente mediante la casella di posta personale e nominativa.

La casella del Servizio/Ufficio è accessibile in modalità di delega previa richiesta e autorizzazione del dirigente. L'accesso alla casella di Servizio/Ufficio in modalità proprietaria per un numero limitato di utenti, va richiesta dal Dirigente al Servizio innovazione, ricerca e transizione digitale.

In caso di assenza dal servizio dell'utente per brevi periodi, è a disposizione apposita funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura.

In caso di assenza non programmata, l'utente può delegare altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al datore di lavoro quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

All'utente non è consentito:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra-aziendali o azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette;
- allegare al testo delle comunicazioni materiale contenente codice eseguibile potenzialmente insicuro (ad es. programmi, scripts, macro), così come file di dimensioni eccessive, (il limite verrà individuato, comunicato ed in caso di necessità aggiornato, dal dirigente del Servizio Innovazione, ricerca e transizione digitale).

L'utilizzo di liste di distribuzione massive che permettono l'invio di messaggi a una parte considerevole o alla totalità degli utenti, è consentito solo a determinati soggetti, su autorizzazione del Direttore generale e previa richiesta del Dirigente; l'invio di messaggi con tali modalità è comunque limitato ai casi in cui il contenuto del messaggio sia effettivamente utile all'intero gruppo.

MONITORAGGIO E CONTROLLI

Le comunicazioni effettuate attraverso il servizio di posta elettronica interno sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte della Amministrazione.

Il traffico da/verso internet può essere automaticamente monitorato in forma elettronica attraverso le registrazioni di sistema (LOG) a cura del Servizio Innovazione, ricerca e

transizione digitale; i dati contenuti nei LOG sono anonimi e tali da precludere l'identificazione degli utenti e/o delle loro attività.

I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Direttore generale per le valutazioni di competenza e riguarderanno per ciascun sito/dominio visitato le seguenti informazioni:

- il numero di utenti che lo visitano
- il numero delle relative pagine richieste
- la quantità di dati da lì scaricati;

L'attivazione di un sistema di registrazione dei dati personali contenuti nei log potrà essere possibile in via eccezionale e tassativamente nelle seguenti ipotesi:

- su richiesta del dipendente nel caso riscontri anomalie nell'accesso a siti/servizi internet nel corso della normale attività di lavoro e l'attivazione del log non anonimo sia necessaria a scopo di analisi
- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- su disposizione del Dirigente responsabile del Servizio Innovazione, ricerca e transizione digitale, d'intesa con il Direttore Generale (salvi i casi di oggettiva impossibilità), quando strettamente necessario per gestire situazioni di pericolo per la sicurezza del sistema stesso (ad es. in caso di pericolo di perdita/compromissione di dati o blocco delle funzionalità).

L'attivazione del sistema di registrazione non anonimo avviene con informazione/comunicazione agli interessati. L'informazione è fornita salvo diversa indicazione dell'autorità giudiziaria richiedente e in maniera preventiva tranne che vi sia urgenza di intervenire. In quest'ultimo caso viene attivata contestualmente o in tempi immediatamente successivi.

I dati personali contenuti nei LOG qualora attivati per le ragioni sopra indicate non sono conservati se non per il tempo strettamente necessario al perseguimento delle rispettive finalità.

I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

Il Dirigente del Servizio Innovazione, ricerca e transizione digitale, in qualità di designato al trattamento dei dati, garantisce il rispetto delle presenti disposizioni.

PUBBLICAZIONE DI CONTENUTI E REALIZZAZIONE DI SITI PERSONALI

L'utente non è autorizzato a produrre e pubblicare propri siti web utilizzando l'infrastruttura informatica comunale. Ogni eventuale necessità di realizzare siti web dovrà essere espressamente autorizzata dal Direttore generale.

L'utente si obbliga a tenere indenne l'Amministrazione da tutte le perdite, danni responsabilità, costi, oneri e spese, ivi comprese le eventuali spese legali, che dovessero essere subite o sostenute quali conseguenze di qualsiasi inadempimento da parte

dell'utente agli obblighi e garanzie previste nel precedente paragrafo o mancato rispetto delle istruzioni fornite dal Servizio Innovazione, ricerca e transizione digitale a tutela della sicurezza del sistema e dei dati e comunque connesse alla diffusione di dati ed informazioni, anche in ipotesi di risarcimento danni pretesi da terzi a qualunque titolo.

INTERRUZIONE E CESSAZIONE D'UFFICIO DEL SERVIZIO

Il Servizio Innovazione, ricerca e transizione digitale può interrompere il servizio di internet e posta elettronica per le manutenzioni ordinarie e straordinarie. Qualora possibile le interruzioni saranno comunicate agli utenti.

Ai sensi del presente disciplinare, l'utilizzo del servizio di accesso ad internet cesserà d'ufficio, previa comunicazione al/agli interessato/i, nei seguenti casi:

- qualora non sussistesse più la condizione di dipendente o collaboratore autorizzato o non fosse confermata l'autorizzazione all'uso;
- qualora venga accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
- qualora vengano sospettate manomissioni e/o interventi sul hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione volontarie imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo IP ed altre informazioni tecniche riservate;
- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti;
- in tutti i casi in cui sussistano situazioni di potenziale pericolo per la sicurezza dell'infrastruttura.