REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI E DEGLI APPARATI DI TELEFONIA

Oggetto: Informativa e autorizzazione all'utilizzo della strumentazione elettronica; informazioni ed istruzioni relative all'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della rete intranet e internet e dello spazio di memorizzazione di dati e documenti.

Premessa

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne dirette ad evitare comportamenti inconsapevoli e/o scorretti. Inoltre, questo regolamento è obbligatorio a partire dal Provvedimento dell'Autorità Garante per la Privacy del 1° marzo 2007 (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e risponde anche all'esigenza di dare una corretta informativa sull'uso dei dati automaticamente ed implicitamente "trattati" a causa dell'uso di un elaboratore.

Autorizzazione

Ai sensi del D.Lgs. n. 196 del 30 giugno 2003, ogni incaricato del trattamento, cui sia stato dato accesso al sistema informativo aziendale mediante credenziali di autenticazione, è autorizzato all'utilizzo della strumentazione elettronica in dotazione (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, etc.) e all'utilizzo della strumentazione telefonica (telefoni a filo, telefoni cordless, telefoni cellulari, compresi smartphone e tablet, ecc.) e del sistema di telefonia in dotazione per lo svolgimento dei compiti assegnati e in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzione ricevute (lettera di incarico, presente regolamento informatico, etc.).

I sistemi informatici aziendali

Il personal computer (fisso o portatile) e i relativi programmi e/o applicazioni affidati al dipendente sono strumenti di lavoro, pertanto:

- devono essere custoditi in modo appropriato;
- possono essere utilizzati solo per fini professionali e non anche per scopi personali, tanto meno per scopi illeciti;
- devono essere prontamente segnalati ai Sistemi Informativi il furto, il danneggiamento o lo smarrimento di tali strumenti.

Accesso al sistema informatico

L'accesso al sistema avviene tramite autenticazione delle credenziali (nome utente e password), pertanto l'utente deve:

- custodire con diligenza le proprie credenziali e non comunicarle ad altre persone;

- provvedere al cambio della password almeno ogni tre mesi (la password deve essere composta da almeno otto caratteri) e, ad ogni cambio, comunicare la nuova password al proprio Responsabile in busta chiusa mediante l'apposito modulo predisposto ed allegato (MOD_PWD);
- bloccare il computer qualora si allontani dalla propria postazione (Ctrl+Alt+Canc Blocca computer su Windows - Logout di Nome Utente su Mac).

Utilizzo del personal computer

Onde evitare il grave pericolo di introdurre virus informatici e spyware, di alterare la stabilità delle applicazioni dell'elaboratore e di incorrere in violazioni delle norme per la tutela dei diritti d'autore, non è consentito:

- installare programmi non autorizzati dai Sistemi Informativi;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; e non è consentito modificare le configurazioni impostate sul proprio computer;
- installare sul proprio computer di mezzi di comunicazione propri (come ad esempio modem e dispositivi bluetooth);
- scaricare files contenuti in supporti magnetici, ottici e per drive USB non aventi alcuna attinenza con la propria prestazione lavorativa;
- memorizzare documenti Informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Tutti i files di provenienza incerta ma attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dei Sistemi Informativi.

Utilizzo della rete aziendale

Le unità condivise di rete sono aree di condivisione d'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; lo stesso vale, in modo specifico, anche per le cartelle "Documenti", "Desktop" e "Scrivania" che, tramite rete, possono essere memorizzate nel server.
L'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisita o installata in violazione del presente regolamento.
E' severamente vietato collegarsi alla rete aziendale utilizzando mezzi propri come, ad esempio, computer portatili, senza esplicita autorizzazione dei Sistemi Informativi.

Utilizzo dei telefoni

I telefoni sono in dotazione per l'uso lavorativo.
In generale, i telefoni non possono essere ceduti nè fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti autorizzati. In particolare, alcuni telefoni sono di uso individuale e non possono essere ceduti né fatti utilizzare neppure ai colleghi.
Il Responsabile della gestione della strumentazione elettronica (d'ora in avanti e per brevità, il Responsabile) può disporre dei telefoni secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.
Il Responsabile è l'unico che può provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso, sui telefoni e più in generale sull'intero sistema telefonico.
In particolare, in modo non esaustivo, si intende stigmatizzare i comportamenti relativi ai seguenti divieti:
Non è consentito modificare le caratteristiche hardware e software impostate sul telefono.

Non è consentita l'installazione di programmi 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.
L'utilizzatore che abbia necessità di apportare modifiche software o hardware al telefono in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta al Responsabile.
Quanto memorizzato sui supporti intereni al telefono potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Responsabile o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.
Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, ecc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dal Responsabile o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

Guasto o furto
In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi al Responsabile a cui è demandata la relativa gestione in queste circostanze.
In caso di furto o smarrimento o danneggiamento dei telefoni, l'utilizzatore deve dare tempestiva comunicazione al Responsabile, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità preposta.
Non è esclusa a priori la responsabilità dell'utilizzatore nel sostenere, anche solo in parte, i costi per la riparazione o sostituzione del telefono.

Dati di traffico e tabulati telefonici
Utilizzando sistemi telefonici per esigenze produttive ed organizzative, è indispensabile l'uso di sistemi evoluti che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2). Tali sistemi registrano le connessioni, ovvero tengono traccia dell'ora, del telefono (e dell'eventuale affidatario) richiedente e della risorsa richiesta e potrebbero eventualmente memorizzare il contenuto della comunicazione. A meno di particolari esigenze tecniche o di sicurezza, circoscritte comunque a periodi di tempo limitati, tali sistemi sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi al traffico ingenerato.
I dati di traffico acquisiti dal sistema di telefonia sono utili per la validazione dei prospetti di consumo che le compagnie telefoniche addebitano, sulla base dei tabulati telefonici da esse riscontrati; pertanto l'operazione di trattamento dei dati di traffico mira principalmente a verificare la sussitenza e la veridicità dei conti telefonici. Potrebbe emergere dall'analisi primaria un interesse ad approfondire la genesi dei costi ed eventualmente a verificare il corretto utilizzo dei telefoni aziendali.
Pertanto, è facoltà del Titolare effettuare controlli mirati all'individuazione di condotte illecite o vietate, ricorrendo sia ai tabulati telefonici, sia ai dati di traffico registrati dal sistema di telefonia interno, mediante operazioni di analisi, selezione e raffronto.

Utilizzo della rete Internet e dei relativi servizi

Navigazione in Internet
Premesso che Internet in azienda è da intendersi prioritariamente come fonte d'informazione per finalità di ricerca, studio e documentazione si precisa che:

- si declina ogni responsabilità per l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, pagamenti con carte di credito e simili;
- non è consentito lo scarico e l'installazione di software gratuiti o in versione di prova (freeware e shareware) prelevati da siti Internet, se non espressamente autorizzati dai Sistemi informativi;
- non è consentito lo scarico di immagini, filmati e files musicali non attinenti all'attività lavorativa ed in violazione delle leggi sul diritto d'autore.

Posta elettronica aziendale

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- le caselle di posta elettronica aziendale assegnate ai dipendenti ed ai collaboratori (caselle del tipo n.cognome@unisg.it) possono essere utilizzate anche per inviare e ricevere messaggi personali;
- la natura della corrispondenza effettuata con le caselle di posta elettronica istituzionali (caselle del tipo nome ufficio@unisg.it) non è privata e non è consentito utilizzare tali caselle per motivi non attinenti allo svolgimento delle mansioni assegnate; i responsabili sono tenuti a controllare la posta in arrivo almeno una volta al giorno e devono delegare una persona di fiducia che possa farlo in caso di propria assenza;
- non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- ogni comunicazione, inviata o ricevuta, che abbia contenuti rilevanti, deve essere visionata od autorizzata dal Responsabile dell'ufficio e per essa, se esterna, si deve fare riferimento alle procedure in essere per la corrispondenza ordinaria;
- tutte le caselle di posta elettronica sono oggetto di salvataggio automatico sia per le comunicazioni in ingresso che in uscita.

Cessazione o sospensione del rapporto di lavoro

Nel caso in cui cessi il rapporto di lavoro o di collaborazione, l'utente incaricato del trattamento deve:

- consegnare i beni aziendali in dotazione (telefono e computer portatili, chiavette USB, etc.)
- copiare i files e i documenti elettronici di rilevanza aziendale sul server.

E' compito dei Sistemi informativi, in seguito alla cessazione di un rapporto di lavoro:

- effettuare il ripristino alla configurazione iniziale (reset) dei beni aziendali dotati di sistema operativo;
- attivare un risponditore automatico sulla casella di posta elettronica precedentemente concessa in uso all'incaricato: tale sistema entrerà in funzione per la durata di 1 mese, salvo accordi diversi, e comunicherà eventuali riferimenti alternativi; al termine del periodo previsto, la casella sarà disattivata;
- disattivare le credenziali di autenticazione sui server.

Controlli e tutela della privacy

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Ai sensi dell'art. 13 del D.Lgs. 30 giugno 2003 n. 196, in conformità a quanto disposto dalla Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- la Direzione, attraverso il proprio Settore Informatico, effettua un monitoraggio periodico dell'hardware e del software installato negli elaboratori aziendali. Tale operazione viene effettuata, in modo completamente automatico per le macchine in rete ed in modo semiautomatico per le macchine stand-alone, mediante l'utilizzo di apposito software installato o da installare in ogni computer aziendale. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati

personali ed i documenti presenti sui computer, ma permette la rilevazione dì software installato in violazione di questo regolamento;

- al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, l'azienda si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il download di files multimediali non attinenti all'attività lavorativa;
- i files contenenti le registrazioni della navigazione sul web sono conservati per 6 mesi come previsto dalle norme in vigore e da esigenze di sicurezza;
- eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate (uffici, servizi) e, solo qualora tali comportamenti dovessero continuare, la Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali;
- nessun controllo viene effettuato sui messaggi di posta elettronica il cui contenuto riguarda forme di corrispondenza assistite da garanzie di segretezza, tutelate anche dalla Costituzione e da norme penali.

Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque elaboratore informatico.
I dati personali saranno trattati nel rispetto delle modalità indicate nell'art. 11, il quale prevede, tra l'altro, che i dati stessi siano trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, esatti, e se necessario aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità del trattamento, nel rispetto delle norme minime di sicurezza previste dall'Allegato B.
I dati potranno essere comunicati in Italia e all'Estero all'interno degli enti collegati con l'Università, a soggetti terzi per incarichi specifici e rispondenti alle finalità del trattamento e nei casi previsti dalla legge.
Gli utenti possono esercitare i diritti di cui all'art. 7, tra cui conferma dell'esistenza, rettifica, integrazione e cancellazione dei dati.
Titolare del trattamento è il Consiglio di Amministrazione dell'Università degli Studi di Scienze Gastronomiche; responsabile del trattamento in oggetto è il Direttore Amministrativo.
La non osservanza del presente regolamento può comportare sanzioni disciplinari, civili e penali.

Pollenzo, 31/03/2011

Per presa visione