



REGOLAMENTO SULL'ORDINAMENTO GENERALE DEGLI UFFICI E DEI SERVIZI

AMMINISTRAZIONE E SICUREZZA DEI SISTEMI INFORMATIVI



TITOLO I IL DIPENDENTE E LA SICUREZZA DEI SISTEMI

Art. 1 Il personal computer in postazione fissa

- 1.1 Il personal computer (d'ora in poi PC) è affidato al dipendente esclusivamente quale postazione fissa per lo svolgimento dell'attività lavorativa.
- 1.2 E' fatto divieto al dipendente di procedere all'attivazione sul PC di una password d'accensione (bios), salvo esplicita e motivata richiesta formale all'Ufficio Sistema Informativo Aziendale.
- 1.3 É fatto divieto al dipendente di apportare modifiche alle caratteristiche hardware e software del PC ad esso assegnato.
- 1.4 É fatto divieto al dipendente di spostare il PC dalla postazione di lavoro di originaria installazione; per esigenze funzionali o di servizio lo spostamento del PC è disposto dal responsabile di Divisione, Agenzia o Progetto ed è eseguito - dietro richiesta - da personale tecnico dell'Ufficio Sistema Informativo Aziendale.
- 1.5 É fatto divieto al dipendente di installare o disinstallare direttamente programmi applicativi sul PC ad esso assegnato; è facoltà del dipendente richiederne l'installazione o la disinstallazione da parte dell'Ufficio Sistema Informativo Aziendale.
- 1.6 Il dipendente è tenuto a mettere in stato di blocco (lock) il PC, ogniqualvolta si allontana dalla postazione e/o dall'ufficio.
- 1.7 Il dipendente è tenuto a spegnere il PC al termine del turno o della giornata di lavoro.
- 1.8 In casi eccezionali o per motivate esigenze di servizio il PC può essere mantenuto acceso, anche oltre il termine del turno o della giornata di lavoro, purché sia messo in stato di blocco (lock).
- 1.9 I dati trattati e archiviati sul PC sono esclusivamente quelli necessari all'attività lavorativa nonché quelli previsti dalla legge e dai regolamenti.
- 1.10 Il dipendente provvede - con cadenza almeno mensile - alla pulizia dei dati archiviati sul PC, nonché alla cancellazione dei file duplicati, obsoleti, inutili o temporanei (ad esempio i files *.tmp).
- 1.11 Il dipendente è responsabile della salvaguardia dei dati archiviati sul PC; a tal fine esegue almeno settimanalmente il salvataggio di una copia dei dati archiviati su adeguati supporti magnetici o su altre postazioni di rete.
- 1.12 La conservazione degli archivi su copie di salvataggio o su altre postazioni di rete va effettuata nel rispetto della normativa sulla protezione dei dati sensibili.
- 1.13 Nella riproduzione o duplicazione di dati del PC il dipendente è tenuto a rispettare i vincoli di legge, le licenze d'uso e i diritti d'autore ad essi associati.

Art. 2 L'accesso alla rete informatica del Comune

- 2.1 Il dipendente è abilitato all'accesso in rete esclusivamente per lo svolgimento dell'attività lavorativa.
- 2.2 L'accesso del dipendente alla rete aziendale è correlato all'identificazione in rete ad esso assegnata.
- 2.3 L'identificazione in rete del dipendente tramite "username" e "password" è di norma personale.

- 2.4 È facoltà dei responsabili di vario livello disporre l'utilizzo di una determinata identità di rete da parte di più di un dipendente; di tali disposizioni è data comunicazione scritta all'Ufficio Sistema Informativo Aziendale.
- 2.5 È vietato l'accesso alla rete con identità di rete ("username" e "password") diversa dalla propria o comunque con identità di rete per cui non si è autorizzati.
- 2.6 È vietato connettere in rete stazioni di lavoro diverse da quelle abilitate dall'Ufficio Sistema Informativo Aziendale.
- 2.7 La creazione su un PC di cartelle condivise con altri dipendenti abilitati all'accesso in rete è soggetta ad autorizzazione preventiva dell'Ufficio Sistema Informativo Aziendale.
- 2.8 È vietato il monitoraggio dei flussi di dati in transito nella rete, salvo che al personale dell'Ufficio Sistema Informativo Aziendale.

Art. 3

L'attivazione di connessioni via modem

- 3.1 La connessione del PC, via modem e linea telefonica, a server o banche dati esterne è soggetta ad autorizzazione preventiva dell'Ufficio Sistema Informativo Aziendale.

Art. 4

Le password

- 4.1 Le password di accesso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite inizialmente dall'Ufficio Sistema Informativo Aziendale.
- 4.2 È fatto obbligo a ciascun dipendente procedere all'immediata sostituzione della password assegnata dall'Ufficio con una password di sua scelta.
- 4.3 Il dipendente è tenuto a conservare nella massima segretezza le password di accesso alla rete ed ai sistemi nonché qualsiasi altra informazione legata al processo di autenticazione.
- 4.4 Il dipendente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato il PC o comunque nel caso in cui non sia in grado di impedire accessi al PC da parte di soggetti non autorizzati.
- 4.5 È fatto obbligo al dipendente sostituire periodicamente le password di cui al comma 4.1 con nuove password.

Art. 5

Il personal computer portatile

- 5.1 Il dipendente è responsabile del PC portatile assegnatogli in via temporanea o permanente ed è tenuto a custodirlo con diligenza sia durante gli spostamenti al di fuori delle sedi comunali, sia durante l'utilizzo nel luogo di lavoro.
- 5.2 Nell'utilizzo del PC portatile il dipendente si attiene alle norme previste per l'utilizzo dei PC in postazione fissa.
- 5.3 Per motivate esigenze di servizio il responsabile di Divisione, Agenzia o Progetto, d'intesa con i Sistemi Informativi, può autorizzare il dipendente all'utilizzo del PC portatile quale postazione di telelavoro abilitata alla connessione via modem con provider Internet.

Art. 6

La posta elettronica

- 6.1 La casella di posta elettronica è assegnata al dipendente esclusivamente per lo svolgimento dell'attività lavorativa.
- 6.2 Il dipendente abilitato all'uso di una casella di posta elettronica è personalmente responsabile del suo corretto utilizzo.
- 6.3 L'attivazione di una nuova casella di posta elettronica personale o multipersonale è richiesta in forma scritta all'Ufficio Sistema Informativo Aziendale dal Responsabile di Divisione, Agenzia o Progetto.
- 6.4 Il dipendente abilitato all'utilizzo di una casella di posta elettronica concorre, con i propri comportamenti, al mantenimento della sicurezza ed efficienza complessiva dei sistemi informativi; in particolare il dipendente si attiene alle seguenti direttive:
 - 6.4.1 cancella senza aprire le e-mail provenienti da mittenti sconosciuti o contenenti messaggi insoliti;
 - 6.4.2 non apre i file allegati ad e-mail provenienti da mittenti conosciuti qualora i file allegati abbiano estensione .exe, .scr, .pif, .bat, .cmd;
 - 6.4.3 non rinvia ad altri indirizzi le e-mail ricevute che invitano a farlo;
 - 6.4.4 evita l'invio di e-mail con file allegati a gruppi troppo numerosi di destinatari interni; in ogni caso allega uno o più file di dimensione complessivamente non superiore 2 MB;
 - 6.4.5 effettua l'invio di e-mail a gruppi numerosi di destinatari interni sostituendo ai file allegati il link ai medesimi, ove reperibili in intranet o internet;
 - 6.4.6 effettua l'invio di e-mail con allegati predisponendoli in formato compresso, con estensione .zip, .rar o .jpg.;
 - 6.4.7 attiva eventuali iscrizioni a "mailing list" esterne solo per motivi inerenti l'attività lavorativa ed il correlato aggiornamento professionale, previa verifica della serietà ed affidabilità del sito di connessione;
 - 6.4.8 assicura regolarmente il riordino delle e-mail ricevute ed inviate, nonché l'eliminazione delle e-mail inattuali o contenenti allegati di grande dimensione.

Art. 7

L'accesso alla rete Internet ed ai relativi servizi

- 7.1 Il dipendente, previa richiesta del Responsabile di Divisione, Agenzia o Progetto, è abilitato all'accesso ad Internet per le esclusive necessità di documentazione poste dallo svolgimento dell'attività lavorativa.
- 7.2 L'accesso, la navigazione e l'utilizzo di servizi in Internet, per motivi diversi da quelli strettamente legati all'attività lavorativa, sono vietati.
- 7.3 Lo scarico da internet di software e programmi applicativi anche gratuiti è effettuabile solo previa autorizzazione dell'Ufficio Sistema Informativo Aziendale

Art. 8

La protezione antivirus

- 8.1 Il dipendente adotta comportamenti atti a ridurre il rischio di intrusioni dall'esterno nei sistemi informativi e di danneggiamenti degli stessi mediante virus o altri software aggressivi; a tal fine il dipendente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus installato sulla propria postazione.

- 8.2 Il dipendente si attiene in particolare alle seguenti direttive:
- 8.2.1 Nel caso in cui il software antivirus rilevi la presenza di un virus che non può essere ripulito, sospende immediatamente ogni elaborazione in corso, senza spegnere il PC e segnala l'accaduto all'Ufficio Sistema Informativo Aziendale.
 - 8.2.2 Verifica ogni supporto magnetico (dvd, cd, chiavi USB, dischetti, ecc.) prima del suo utilizzo mediante il programma antivirus e, nel caso venga rilevato un virus non eliminabile, rinuncia all'utilizzo dello stesso.

TITOLO II

L'AMMINISTRAZIONE DEI SISTEMI

Art. 9

Le funzioni di controllo

- 9.1 L'Ufficio Sistema Informativo Aziendale predispone dispositivi e procedure tecniche atti ad assicurare e a monitorare il regolare funzionamento dei sistemi informativi; a tal fine formula proposte di procedure e di piani per la sicurezza volti alla salvaguardia delle basi di dati, delle parti hardware e software, nonché delle connessioni di rete che compongono i sistemi informativi.
- 9.2 La Direzione Generale, su proposta dell'Ufficio Sistema Informativo Aziendale, approva le procedure e i piani per la sicurezza dei sistemi.
- 9.3 In attuazione dei piani di cui ai commi precedenti l'Ufficio Sistema Informativo Aziendale individua tra il proprio personale tecnico uno o più dipendenti incaricati delle funzioni di amministrazione, controllo e di help-desk per la sicurezza dei sistemi.
- 9.4 I dipendenti incaricati delle funzioni di amministrazione e controllo per la sicurezza dei sistemi provvedono al loro regolare monitoraggio; nello svolgimento di tale funzione gli stessi si attengono alle seguenti direttive:
 - 9.4.1 Assicurano il rispetto della normativa sulla privacy e sulla protezione dei dati sensibili in relazione a contenuti ed informazioni accessibili nei sistemi.
 - 9.4.2 Assicurano il rispetto delle garanzie e dei limiti previsti dallo Statuto dei Lavoratori in materia di controllo a distanza delle attività lavorative con mezzi audiovisivi.
 - 9.4.3 Prendono nota e riferiscono al proprio responsabile, riguardo ai comportamenti dei dipendenti che contrastino - sotto il profilo disciplinare - con le norme di cui al Titolo I del presente Regolamento, ovvero che ravvisino violazioni di norme di legge in materia di telecomunicazioni, di danno alla pubblica amministrazione, di segreto d'ufficio, di tutela della privacy, di proprietà intellettuale e di diritto d'autore.
 - 9.4.4 Effettuano, previa comunicazione ai dipendenti interessati, tutti gli interventi tecnici di ripristino della sicurezza dei sistemi, anche mediante assunzione del controllo da remoto di postazioni singole, nonché di unità di rete, ove interessate da rischio per la sicurezza.
- 9.5 Il Responsabile dell'Ufficio Sistema Informativo Aziendale riferisce periodicamente alla Direzione Generale circa lo stato complessivo del sistema informativo, anche alla luce delle attività di monitoraggio di cui al presente articolo.

TITOLO III

INOSSERVANZA DEL REGOLAMENTO E NORME FINALI

Art. 10

Le violazioni di norme regolamentari e di legge

- 10.1 La Direzione Generale, visti gli esiti dei controlli di cui al precedente art. 9, ove riscontri gli estremi di eventuali violazioni di norme del presente regolamento, ovvero gli estremi di violazioni di norme di legge, sentite la Divisione Risorse Umane e la Divisione Autonoma Avvocatura Comunale, dà avvio ai procedimenti conseguenti.

Art. 11

I sistemi informativi e l'attività sindacale

- 11.1 In deroga ai limiti di cui presente regolamento, il dipendente con incarico sindacale può avvalersi dei sistemi informativi comunali anche ai fini di un più efficace svolgimento del proprio ruolo di rappresentanza e tutela del personale dipendente.
- 11.2 L'utilizzo delle risorse dei sistemi informativi per lo svolgimento dell'attività sindacale avviene nel rispetto delle priorità poste dal buon funzionamento degli uffici e dei servizi e delle norme vigenti.

Art. 12

L'aggiornamento e la revisione del regolamento

- 12.1 Le modifiche, integrazioni e revisioni del presente Regolamento sono disposte dalla Giunta su proposta del Direttore Generale.

INDICE

TITOLO I – IL DIPENDENTE E LA SICUREZZA DEI SISTEMI

Art. 1 - Il personal computer in postazione fissa	pag. 1
Art. 2 - L'accesso alla rete informatica del comune	pag. 1
Art. 3 - L'attivazione di connessioni via modem	pag. 2
Art. 4 - Le password	pag. 2
Art. 5 - Il personal computer portatile	pag. 2
Art. 6 - La posta elettronica	pag. 3
Art. 7 - L'accesso alla rete Internet ed ai relativi servizi	pag. 3
Art. 8 - La protezione antivirus	pag. 3

TITOLO II – L'AMMINISTRAZIONE DEI SISTEMI

Art. 9 - Le funzioni di controllo	pag. 4
-----------------------------------	--------

TITOLO III – INOSSERVANZA DEL REGOLAMENTO E NORME FINALI

Art. 10 - Le violazioni di norme regolamentari e di legge	pag. 5
Art. 11 - Sistemi informativi e attività sindacale	pag. 5
Art. 12 - L'aggiornamento e la revisione del regolamento	pag. 5