DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEL PERSONALE DELL'ACI

Art. 1
Oggetto, finalità ed ambito di applicazione

1. Il presente Disciplinare regolamenta l'utilizzo degli strumenti informatici (postazioni di lavoro fisse e mobili, posta elettronica, Internet ed Intranet) che l'ACI mette a disposizione del personale e si pone la finalità di garantire la *privacy* dei dipendenti e prevenire usi indebiti degli stessi strumenti, in conformità alle indicazioni e linee guida fornite dall'Autorità garante per la *privacy* con il Provvedimento 1° marzo 2007.

2. Il presente Disciplinare si applica a tutto il personale in servizio presso l'Ente, con qualifica dirigenziale e non dirigenziale. Le disposizioni che seguono si estendono, in quanto compatibili, a tutti coloro che, in qualità di utenti esterni, gestiscono ed utilizzano gli strumenti informatici forniti dall'Ente, sulla base di un rapporto di lavoro, di stage o tirocinio ovvero di fornitura o appalto di servizi.

Art. 2
Prescrizioni interne sulla sicurezza dei dati e dei sistemi

1. L'ACI, in conformità all'art. 34 del decreto legislativo 30 giugno 2003 n° 196 ("Codice in materia di protezione dei dati personali"), adotta un sistema di identificazione e di autorizzazione con il quale vengono riconosciuti e profilati gli utenti del proprio sistema informativo.

2. L'ACI stabilisce inoltre le seguenti prescrizioni interne, in linea con quanto previsto nell'Allegato B al d. lgs. n° 196/2003, in materia di misure minime di sicurezza:

a) ad ogni dipendente in servizio è assegnata una postazione di lavoro fissa; è facoltà dell'Amministrazione assegnare postazioni mobili, anche in alternativa alla postazione fissa; è responsabilità del dipendente usare le postazioni informatiche di lavoro in modo protetto ed esclusivamente per motivi di lavoro;

b) l'accesso alla postazione di lavoro è controllata da un codice segreto (*password*), in alcuni casi accompagnato da un codice utente (*user-id*), utilizzabili solo dall'utente e generati nel rispetto delle norme sui criteri minimi di sicurezza;

c) il predetto codice (*password*) deve essere inserito con le cautele necessarie per conservarne la segretezza e deve essere periodicamente modificato dall'utente almeno ogni tre mesi; la *password* deve essere composta da un numero minimo di otto caratteri, non deve determinare associazioni logiche interpretabili o riconoscibili da estranei in quanto riferite a caratteristiche note del titolare, deve essere priva di ripetizioni consecutive di caratteri e deve contenere indifferentemente maiuscole e minuscole, lettere, numeri e caratteri speciali, qualora l'applicazione lo consenta;

d) l'accesso alla postazione di lavoro deve essere bloccato ogni qual volta ci si allontani da essa (digitando sulla tastiera "CTRL+ALT+CANC");

e) qualsiasi operazione effettuata attraverso l'inserimento di credenziali identificate dal sistema informatico di riconoscimento (quale il codice utente associato alla parola chiave riservata) viene ricondotta al titolare delle medesime credenziali, indipendentemente dalla postazione di lavoro utilizzata, salvo che lo stesso titolare delle credenziali non fornisca prova contraria;

f) nessun dispositivo componente la postazione di lavoro può essere rimosso, salvo specifica autorizzazione dell'amministratore di sistema; ogni collegamento con installazioni esterne ad ACI deve essere autorizzato dal Responsabile della Sicurezza ICT, tenuto conto del livello di rischio di sicurezza associato;

g) non è consentito al personale la modifica delle caratteristiche *hardware* e *software* impostate sulla postazione di lavoro, salvo autorizzazione esplicita dell'amministratore di sistema;

h) in caso di furto o smarrimento di strumenti informatici dell'Amministrazione, il dipendente al quale gi stessi strumenti sono affidati, oltre che denunciare l'accaduto all'Autorità di Pubblica Sicurezza, deve tempestivamente darne comunicazione al Direttore o Responsabile di Struttura di riferimento, che la trasmette alla Direzione Sistemi Informativi (DSI);

i) ogni dipendente è tenuto ad assumere comportamenti tali da ridurre il rischio di attacco al sistema informativo aziendale; è obbligatorio controllare costantemente la presenza e il regolare funzionamento del *software* antivirus aziendale e sospendere le attività in presenza di *software* malevoli (cd. *malware*) informando tempestivamente, in caso di Strutture periferiche, l'esperto informatico della DSI (di riferimento sul territorio) o, in caso di Strutture centrali, la Funzione Sicurezza della stessa DSI e/o l'amministratore di sistema;

j) in caso di assenza improvvisa o prolungata del dipendente, qualora il Direttore o Responsabile di Struttura di riferimento ne ravvisi urgenza e necessità, lo stesso Direttore o Responsabile può accedere ai dati aziendali presenti nella postazione di lavoro del dipendente assente; a tal fine, deve essere rivolta specifica richiesta al Sistema Informativo e si devono seguire le modalità previste nell'appendice alle "Politiche di Sicurezza delle Informazioni" per il caso di cui alla lett. j) del successivo art. 5 (in tema di caselle di posta elettronica nominativa). Sono comunque fatte salve le particolare garanzie, previste nello stesso art. 5 del presente Disciplinare, per l'accesso ai messaggi di posta elettronica nominativa.

Art. 3
Accesso ed utilizzo di Internet

1. L'ACI consente l'accesso ad Internet a tutti i dipendenti della Strutture centrali e periferiche promuovendo la digitalizzazione delle attività e dei servizi dell'Amministrazione.

2. Internet e i servizi di rete devono essere utilizzati esclusivamente per fini lavorativi. L'ACI stabilisce, inoltre, le seguenti prescrizioni interne finalizzate ad un corretto utilizzo degli stessi Internet e servizi di rete:

a) è consentita l'effettuazione di adempimenti *on line* nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici, o per tenere rapporti con istituti bancari e assicurativi, nei tempi strettamente necessari allo svolgimento delle transazioni, come indicato nella Direttiva n° 2 del 26 maggio 2009 emanata dal Ministro per la Pubblica Amministrazione e l'Innovazione;

b) il Sistema Informativo predispone quanto necessario per l'applicazione di particolari prodotti di filtraggio (*URL filtering*) ad ogni postazione di lavoro, presso le Strutture centrali e periferiche, allo scopo di impedire l'accesso ad una serie di siti non pertinenti, utilizzando *black list* di siti non consultabili *a priori* – quali, ad esempio, siti pornografici e siti contenenti attività ludiche - sulla base di elenchi precostituiti ed aggiornati da società fornitrici specializzate;

c) è vietato "scaricare" o "prelevare" dalla rete Internet (cd. *download) file* musicali o multimediali, se non previa autorizzazione del Sistema Informativo che, di norma, sarà rilasciata al personale che svolge attività di carattere informatico;

d) sono altresì vietate operazioni di invio di *file* alla rete Internet (cd. *upload*);

e) il personale è tenuto al rispetto della regolamentazione sul diritto d'autore, per quanto riguarda eventuali programmi scaricati dalla rete Internet.

Art. 4
"Portale della comunicazione interna", altri strumenti di comunicazione interna e pubblicità degli atti dell'Ente

1. L'ACI, ai sensi dell'art. 47 c. 3 del decreto legislativo 7 novembre 2005 n° 54 ("Codice dell'amministrazione digitale"), utilizza per le comunicazioni tra l'Amministrazione ed i propri dipendenti la posta elettronica e gli altri strumenti informatici attivati dalla stessa Amministrazione, quali il Protocollo informatico e l'Intranet aziendale denominata "Portale della comunicazione interna".

2. ACI assicura la conoscenza degli atti di interesse generale del personale adottati dall'Amministrazione attraverso la pubblicazione degli stessi sul "Portale della Comunicazione Interna".

3. Il personale in servizio è tenuto ad accedere al "Portale della comunicazione interna" ed a prendere visione dei documenti pubblicati, con la frequenza necessaria per tenersi tempestivamente e costantemente aggiornato sulle attività dell'Ente e sulle comunicazioni che l'Amministrazione indirizza ai dipendenti. In caso di assenza dal servizio, il personale riceve comunicazioni alternative, tali da assicurare la tempestiva conoscenza dei predetti atti di interesse generale.

4. Il personale in servizio, al quale è inviata o assegnata la corrispondenza di interesse attraverso il Protocollo informatico dell'Ente, è tenuto alla consultazione della stessa corrispondenza con la frequenza richiesta per il tempestivo espletamento delle attività lavorative.

Art. 5
Utilizzo della posta elettronica nominativa

1. L'ACI fornisce a ciascun dipendente in servizio presso le Strutture centrali e periferiche un indirizzo di posta elettronica nominativo esposto ad Internet. Gli elenchi degli indirizzi di posta elettronica dei dipendenti non possono essere forniti a soggetti esterni all'Amministrazione, salvo che per specifiche finalità individuate dalla Direzione competente e appositamente autorizzate con provvedimento motivato.

2. L'indirizzo di posta elettronica deve essere utilizzato dal personale esclusivamente per fini di lavoro e per contattare le Organizzazioni sindacali rappresentative e le RSU della Struttura di appartenenza. L'ACI stabilisce, inoltre, le seguenti prescrizioni interne finalizzate ad un corretto utilizzo della stessa posta elettronica nominativa:

a) non è consentito utilizzare la posta elettronica per ragioni personali; sono proibiti utilizzi impropri quali l'invio di messaggi diffamatori, osceni, di profanazione, lettere minatorie o di offesa razziale, messaggi commerciali o di propaganda, le cosiddette "catene di S. Antonio" nonché l'utilizzo della posta elettronica con modalità di *forum*;

b) il personale, nelle comunicazioni a mezzo posta elettronica con i vari livelli organizzativi dell'Ente, deve rispettare, di norma, gli ordinari riporti amministrativi; in ogni caso, ciascun dipendente è tenuto ad utilizzare un linguaggio appropriato ed una forma espositiva adeguata, secondo il comune sentire;

c) l'invio di messaggi di posta elettronica ad un elevato numero di destinatari è consentito solo qualora richiesto da specifiche esigenze di lavoro; è fatto salvo, in ogni caso, l'invio di circolari o analoghi messaggi usualmente indirizzati a tutto il personale o a specifici gruppi di posta;

d) si applicano all'utilizzo della posta elettronica le ordinarie regole di riservatezza e di segreto per ragioni d'ufficio; i documenti di lavoro possono essere inviati ad indirizzi di posta elettronica esterni solo se necessario per l'attività lavorativa;

e) tramite l'indirizzo di posta elettronica possono essere inviati *file* allegati; l'invio deve essere commisurato alla capacità delle infrastrutture adottate al fine di non causare l'indisponibilità dei sistemi e dei dati, secondo quanto disposto delle istruzioni operative fornite in appendice alle "Politiche di Sicurezza delle Informazioni";

f) il personale è tenuto a non aprire *file* allegati di incerta provenienza e dalla dubbia o doppia estensione (ad esempio: .exe; .jpg.pif; ecc.), se non dopo aver contattato la Funzione Sicurezza DSI per i controlli del caso;

g) il personale è tenuto a non dare seguito a messaggi con dubbi oggetti e provenienza in cui vengano richieste informazioni riguardanti dati personali e/o credenziali di autenticazione, se non dopo aver contattato la Funzione Sicurezza DSI per i controlli del caso;

h) ciascun dipendente ha a disposizione una funzionalità che consente di inviare automaticamente, in caso di assenza, messaggi di risposta contenenti i riferimenti di posta elettronica o telefonici di altro dipendente a cui potrà rivolgersi il richiedente per particolari informazioni ("*Outlook*/ Strumenti/ Regole fuori sede");

i) ciascun dipendente può delegare un altro dipendente quale "fiduciario", al fine di verificare i contenuti dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate alla attività lavorativa; l'accesso ai predetti messaggi avviene - con le modalità stabilite nelle istruzioni operative in appendice alle "Politiche di sicurezza delle Informazioni" - attraverso il Sistema Informativo, al quale il "fiduciario" deve rivolgere specifica richiesta; con la delega il "fiduciario" è autorizzato ad inoltrare al Direttore o Responsabile di Struttura di riferimento i messaggi ritenuti rilevanti per lo svolgimento dell'attività lavorativa; di tale attività il "fiduciario" è tenuto a dare informativa, alla prima occasione utile, al dipendente interessato;

j) in caso di contemporanea assenza del dipendente delegante e del "fiduciario", ovvero nel caso in cui non sia stata rilasciata alcuna delega, e sussistendo urgenza e comprovata necessità, la casella di posta elettronica può essere visionata, con le stesse modalità indicate alla lettera precedente, dal Direttore o Responsabile di Struttura di riferimento del dipendente interessato; di tale eventualità deve essere data informativa al predetto dipendente;

k) il Sistema Informativo dell'Ente provvede ad inserire in automatico, in calce ad ogni comunicazione inviata via *e-mail* all'esterno dagli indirizzi nominativi, un messaggio contenente l'avvertenza che indichi ai destinatari degli stessi messaggi la natura non personale del contenuto di questi ultimi e la possibilità che il relativo contenuto possa essere comunicato all'interno dell'Amministrazione;

l) ciascun dipendente, in caso di cessazione del rapporto di lavoro, è tenuto ad eliminare i messaggi di posta elettronica il cui contenuto non ritenga utile per assicurare la continuità funzionale delle attività svolte; in ogni caso il Sistema Informativo dell'Ente provvederà ad archiviare la corrispondenza memorizzata sui *server* aziendali, secondo le modalità e i tempi stabiliti dalle istruzioni operative in appendice alle "Politiche di Sicurezza delle Informazioni".

Art. 6
Utilizzo della posta elettronica condivisa

1. Per esigenze lavorative l'ACI può disporre l'utilizzo di caselle di posta elettronica esposte ad Internet condivise da più dipendenti di Strutture centrali, attraverso le quali gli utenti esterni dei servizi ACI possono interfacciarsi con l'Amministrazione (ad esempio info@aci.it), ovvero può disporre l'utilizzo di caselle di posta elettronica condivise presso le Strutture periferiche, attraverso le quali gli utenti possono interfacciarsi localmente con le stesse Strutture.

2. L'ACI, per particolari esigenze lavorative, istituisce caselle di posta elettronica condivise interne (ad esempio, "dsifunzionesicurezza") al fine di garantire assistenza, formazione, regolamentazione ed informazione su particolari tematiche di interesse dell'Amministrazione.

3. L'ACI, fermo restando l'applicazione delle prescrizioni di cui al precedente art. 5, stabilisce le seguenti ulteriori prescrizioni interne finalizzate ad un corretto utilizzo della posta elettronica condivisa:

a) il dipendente che risponde alle richieste avanzate attraverso le caselle di posta condivise dovrà apporre in calce alle stesse la propria sigla, al fine di garantire la massima trasparenza per l'utente;

b) le risposte fornite tramite le caselle di posta elettronica condivise possono essere consultate da ciascun dipendente che abbia l'accesso alla stessa casella di posta;

c) le risposte fornite sono archiviate con le stesse modalità e gli stessi tempi previsti per le caselle di posta elettronica nominativa.

Art. 7
Controlli sull'utilizzo di Internet e della posta elettronica

1. L'ACI adotta idonei strumenti di controllo graduato, atti a indirizzare i singoli dipendenti verso un uso corretto e pertinente della posta elettronica e di Internet.

2. Con la periodicità stabilita dalle istruzioni operative in appendice alla "Politiche di Sicurezza delle Informazioni", la Funzione Sicurezza della DSI provvede ad attivare forme di controllo anonimo, preliminarmente su dati aggregati, riferiti a specifiche aree lavorative o strutture organizzative.

3. A fronte di un rilevato utilizzo anomalo, il controllo può concludersi con un avviso generalizzato avente come scopo quello di invitare i dipendenti ad attenersi scrupolosamente alle istruzioni impartite circa l'utilizzo degli strumenti di lavoro.

4. In caso di successivi ripetuti utilizzi anomali, saranno effettuati controlli individuali sui dipendenti afferenti alle specifiche aree lavorative o strutture organizzative coinvolte, previa comunicazione ai soggetti sindacali di cui all'art. 8 c. 2 del CCNL 16 febbraio 1999 (Organizzazioni sindacali rappresentative ed RSU) ed agli stessi dipendenti interessati al controllo.

Art. 8
Sanzioni e responsabilità

1. Il mancato rispetto o la violazione delle regole contenute negli articoli da 1 a 6 del presente Disciplinare è perseguibile con le sanzioni disciplinari previste dalla contrattazione collettiva, nonché con le azioni civili, penali e contabili previste dalla legge vigente.