



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

Prot. n.P. 17105

Cagliari, 28 giugno 2013

> A tutti i dipendenti della Direzione generale

Oggetto: Regolamento per l'utilizzo della rete informatica e telematica e dei servizi informatici della Direzione generale del Personale.



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

INDICE

Premessa	3
CAPO I – FINALITA', AMBITO DI APPLICAZIONE, PRINCIPI GENERALI	3
Art. 1 - Oggetto e ambito di applicazione	3
Art. 2 - Principi generali	4
Art. 3 – Composizione del sistema informatico della Direzione generale	4
CAPO II – CRITERI E VINCOLI DI UTILIZZO DEGLI STRUMENTI INFORMATICI	5
Art. 4 - Modalità di utilizzo del sistema informatico	5
Art. 5 - Credenziali di accesso al sistema informatico	6
Art. 6 – Utilizzo di PC portatili e conservazione supporti rimovibili	7
6.1. <i>Utilizzo di PC portatili</i>	7
6.2. <i>Utilizzo e conservazione dei supporti rimovibili</i>	7
Art. 7 - Servizi di rete	8
7.1. <i>Cartelle condivise</i>	8
7.2. <i>Antivirus</i>	9
7.3. <i>Aggiornamento e distribuzione del software</i>	9
7.4. <i>Internet</i>	9
7.5. <i>Posta elettronica</i>	10
CAPO III – ASSISTENZA E SERVIZI	11
Art. 8 - Procedure operative	11
CAPO IV – CONTROLLI e responsabilita'	11
Art. 9 - Controlli, responsabilità e sanzioni	11
Art. 10 - Responsabilità dell'amministratore di sistema	12
CAPO V – INFORMATIVA	12
Art. 11 - Entrata in vigore del regolamento	12
ALLEGATO A – Modulo di presa visione e accettazione del regolamento	13
ALLEGATO B - Glossario	17



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

PREMESSA

Le realtà lavorative della pubblica amministrazione, sono andate caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche che, se da un lato hanno consentito l'introduzione di innovative tecniche gestionali, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti ai propri collaboratori per lo svolgimento delle mansioni e compiti affidati.

Si rende pertanto necessario adottare adeguati sistemi di controllo sull'utilizzo di tali strumenti e sanzionare conseguentemente quegli usi scorretti che, oltre ad essere contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile, espongono l'Amministrazione regionale a rischi tanto patrimoniali quanto penali.

I controlli sull'uso degli strumenti informatici tuttavia, tendono a garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro il cui uso a fini personali è precluso, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy.

Il presente regolamento sull'utilizzo delle risorse ICT nell'ambito della Direzione Generale del personale, oltre a dettare una disciplina per l'utilizzo degli strumenti informatici di uso quotidiano, vuole costituire un utile strumento per sensibilizzare il personale su aspetti altrettanto importanti nella gestione dei sistemi locali.

CAPO I – FINALITA', AMBITO DI APPLICAZIONE, PRINCIPI GENERALI

ART. 1 - OGGETTO E AMBITO DI APPLICAZIONE

Il presente regolamento disciplina le modalità di accesso e di utilizzo della rete informatica e telematica della Direzione generale del Personale e dei servizi che, tramite la stessa rete, è possibile utilizzare.

Il regolamento si applica a tutti i dipendenti "utenti", senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori della Direzione generale a prescindere dal rapporto contrattuale con la stessa intrattenuto (personale in comando, collaboratore a progetto, stagisti, ecc.).

Per "utente" deve intendersi chiunque possieda specifiche credenziali di autenticazione.

Il regolamento ha lo scopo di:

1. stabilire le regole di accesso al sistema degli utenti autorizzati;
2. informare gli utenti sui vincoli e le potenzialità del sistema e sugli eventuali rischi connessi all'uso indebito dei mezzi elettronici;
3. illustrare le azioni per garantire la riservatezza delle informazioni e dei dati trattati e per rendere efficiente e sicuro il sistema informatico della Direzione generale;
4. promuovere un impiego ottimale delle risorse al fine di semplificarne l'uso e realizzare condizioni di efficienza, efficacia e sicurezza per gli utenti;



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

5. indicare i servizi informatici e telematici disponibili sul sistema tecnologico in dotazione e le modalità d'uso.

ART. 2 - PRINCIPI GENERALI

La Regione autonoma della Sardegna promuove l'utilizzo degli strumenti informatici, di internet e della posta elettronica quali mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati in materia dalla normativa vigente.

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, con particolare riferimento ai servizi, ai programmi a cui ha accesso e ai dati trattati a fini istituzionali.

E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.

Il lavoratore deve custodire ed utilizzare gli strumenti informatici, internet, la posta elettronica in modo appropriato e diligente ed è responsabile della propria postazione di lavoro.

Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Amministrazione regionale e più nello specifico, alla Direzione generale.

ART. 3 – COMPOSIZIONE DEL SISTEMA INFORMATICO DELLA DIREZIONE GENERALE

- a. Tutte le attrezzature informatiche sia hardware che software (server e pc completi di software di base ed applicativo, stampanti e dispositivi informatici di ogni natura) e i dispositivi di rete e impiantistica (cablaggi e armadi) dislocate presso le sedi di Viale Trieste 190 e di Via XXIX Novembre 29 (FITQ), incluse quelle fornite dall'Assessorato degli enti locali o acquistate dai singoli servizi della stessa Direzione, complete della relativa documentazione identificativa, sono prese in carico dal Settore SI (incardinato nel Servizio organizzazione, formazione, reclutamento e mobilità) e rappresentano il *sistema informatico* della Direzione generale.
- b. L'assegnazione delle postazioni di lavoro, gestite direttamente dal Settore SI, avviene normalmente, con criteri legati alle necessità operative individuali ed alle disponibilità di stazioni di lavoro; su specifica richiesta del Direttore generale o dei Dirigenti responsabili dei servizi possono essere concordati criteri e priorità di assegnazione differenti da quelle generalmente applicate.
- c. Le postazioni sono assegnate "temporaneamente" agli utenti. In caso di trasferimento il Settore SI individua una postazione di lavoro adeguata da consegnare al dipendente per l'ufficio di destinazione - così come stabilito del Servizio provveditorato della Direzione generale degli Enti Locali - sebbene non coincidente con quella utilizzata fino a quel momento.
- d. Le postazioni di lavoro dei dipendenti trasferiti definitivamente o temporaneamente presso la Direzione generale, previa inventariazione da parte del consegnatario, entrano a far parte del sistema informatico della Direzione generale e, come tali, configurate secondo quanto previsto dal presente regolamento.
- e. Sono escluse dal sistema informatico della Direzione generale, le postazioni installate presso l'Ufficio di gabinetto dell'Assessore degli affari generali. Su specifica richiesta del Capo di gabinetto, le postazioni potranno essere inserite nel dominio della Direzione generale per



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

usufruire di tutti i servizi di rete disponibili, previa accettazione da parte degli utenti individuati, delle disposizioni previste dal presente regolamento (Allegato A); in alternativa a tale soluzione, detta struttura potrà disporre dei servizi tecnologici di rete amministrati dalla Direzione generale degli affari generali e società dell'informazione.

- f. Il sistema informatico prevede l'uso di server dislocati presso la sala operativa telematica situata al 2° piano del palazzo di Viale Trieste 190. L'accesso alla sala e ai locali degli apparati di rete è consentito unicamente al personale autorizzato. L'accesso da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo alla presenza di un incaricato.

CAPO II – CRITERI E VINCOLI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

ART. 4 - MODALITÀ DI UTILIZZO DEL SISTEMA INFORMATICO

Durante l'espletamento della propria attività lavorativa, i dipendenti devono attenersi alle seguenti regole e raccomandazioni:

- a. Il Personal Computer (PC) affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il PC deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
- b. Il PC permette l'accesso alla rete della Amministrazione regionale solo attraverso specifiche credenziali di autenticazione come descritto nel successivo articolo 5.
- c. Il sistema informatico è disponibile dal lunedì al venerdì dalle 7:00 alle 21:00, sabato e domenica esclusi. Ove si rendesse necessario un accesso in giornate e orari diversi da quelli specificati, previa autorizzazione del proprio Dirigente, dovrà essere inviata la preventiva richiesta all'amministratore di sistema all'indirizzo: admin.DGpers@regione.sardegna.it.
- d. Prima di lasciare gli uffici o in caso di assenze prolungate durante l'orario di lavoro il PC deve essere sempre spento o protetto con blocca schermo: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
- e. Gli utenti sono autorizzati ad accedere al sistema informatico soltanto durante la *effettiva presenza in servizio*¹ nella sede di lavoro; per garantire la sicurezza degli accessi, l'amministratore di sistema è autorizzato a disconnettere le sessioni di collegamento che non rispettano tale raccomandazione.
- f. Non è consentita la memorizzazione di file audio, video e foto sul disco rigido del PC assegnato se non attinente la attività lavorativa.
- g. L'amministratore di sistema, è autorizzato a compiere interventi diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). La stessa facoltà si applica anche in caso di assenza prolungata od impedimento dell'utente previa informazione al Dirigente responsabile.

¹ Per effettiva presenza in servizio si intende la corrispondenza di accesso al sistema informatico rispetto alla presenza nell'edificio, certificata attraverso le timbrature effettuate sul sistema di rilevazione presenze.



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

- h. L'amministratore di sistema può collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale operatività nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento, generalmente, avviene su richiesta dell'utente. In caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico, l'intervento sarà eseguito con la doverosa tempestività e successivamente ne sarà data comunicazione all'utente interessato.
- i. Non è consentito l'uso di programmi diversi da quelli installati dall'amministratore né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. Le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Regione.
- j. Salvo preventiva espressa autorizzazione dell'amministratore di sistema, non è consentito modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (hard-disk, DVD, fotocamere, apparati multimediali, ecc).
- k. Ciascun utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Settore SI nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 7.2. relativo alle procedure di protezione antivirus.
- l. Per evitare il pericolo di introdurre virus informatici nella rete locale, devono essere utilizzati esclusivamente programmi distribuiti dall'Amministrazione regionale; in particolare è vietato scaricare files e software anche gratuiti se non dopo espressa autorizzazione del proprio Dirigente, in accordo con il Settore SI.
- m. Gli applicativi SAP sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la normativa vigente sulla privacy (vedi dlgs 196/2003 e successive modificazioni).
- n. Non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- o. Non è consentito duplicare e/o cedere programmi e altro materiale informatico, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati.
- p. Nessun elemento hardware del sistema (PC, workstation, server, stampanti, etc.) può essere disconnesso dalla rete senza l'autorizzazione preventiva del Settore SI se non in presenza di un pericolo oggettivo per le persone o le cose.

ART. 5 - CREDENZIALI DI ACCESSO AL SISTEMA INFORMATICO

- a. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'amministratore di sistema che agisce per delega del Direttore generale.
- b. Il rilascio delle autorizzazioni avviene sulla base di motivata formale richiesta del Dirigente della struttura nel quale è incardinato il nuovo utente.



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

- c. Le credenziali sono costituite da un codice identificativo personale (username o user id) e da una parola chiave (password) da utilizzarsi esclusivamente sul PC assegnato. E' fatto divieto dell'uso di dette credenziali su computer non assegnati all'utente.
- d. La password non deve contenere riferimenti agevolmente riconducibili all'utente. Essa deve essere modificata al primo utilizzo e periodicamente ai sensi della normativa in vigore, secondo la procedura di modifica proposta automaticamente dal sistema.
- e. Le credenziali di autenticazione sono strettamente personali e in nessun caso cedibili. Ogni utente è responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali (v. dlgs 196/2003 e s.m.i.). Le credenziali sono da intendersi a tempo determinato e decadono al termine delle attività che le aveva giustificate senza bisogno di preavviso.
- f. L'utente non deve utilizzare account diverso da quello assegnatogli allo scopo di mascherare la propria identità, o comunque operare in modo da eludere i controlli di sicurezza esistenti.
- g. L'utente si impegna a non sfruttare eventuali debolezze di sicurezza o anomalie del sistema di cui venisse a conoscenza e al contempo si impegna a segnalarle in forma riservata all'amministratore di sistema.
- h. Ogni utente deve contribuire alla sicurezza complessiva del sistema informatico, ed è responsabile civilmente e penalmente del corretto uso delle risorse e dei servizi ai quali ha accesso e dei propri dati di competenza.
- i. L'utente viene informato, nel rispetto del D.lgs. 196/2003 "Codice in materia di protezione dei dati personali", che il suo operato sulle attrezzature assegnate e il suo traffico in rete possono essere monitorati, registrati e resi disponibili all'autorità competente. L'utilizzo del sistema informatico deve essere razionale e rispondente alla normativa vigente, evitando comportamenti che mettano in pericolo l'integrità e la funzionalità del sistema stesso.

ART. 6 – UTILIZZO DI PC PORTATILI E CONSERVAZIONE SUPPORTI RIMOVIBILI

6.1. Utilizzo di PC portatili

- a. L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante l'utilizzo nel luogo di lavoro sia durante gli spostamenti.
- b. Ai PC portatili si applicano le regole previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della restituzione.

6.2. Utilizzo e conservazione dei supporti rimovibili

- a. I supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni riservate, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
- b. Per assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del settore SI e seguire le istruzioni da questo impartite.
- c. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere, dagli utenti, adeguatamente custoditi in armadi chiusi.



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

- d. E' vietato l'utilizzo di supporti rimovibili personali.
- e. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

ART. 7 - SERVIZI DI RETE

7.1. *Cartelle condivise*

- a. Per l'accesso alla rete della Direzione generale ciascun utente deve essere in possesso della specifica credenziale di autenticazione assegnata dall'amministratore di sistema, come specificato al precedente articolo 5.
- b. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.
- c. Tutti gli utenti possono usufruire, sulla rete locale, dell'utilizzo di 3 tipologie di cartelle condivise dislocate nel server centrale di sede denominato DFS:

- *cartelle di struttura*
- *cartelle di backup*
- *cartelle di procedimento.*

Le autorizzazioni di accesso alle *cartelle di struttura* consentono una condivisione, fra utenti della stessa struttura (servizi e/o settori), di documenti che vengono depositati sul server di rete e resi accessibili dalle diverse postazioni di lavoro a seconda dell'effettiva appartenenza dei singoli utenti alla struttura di riferimento.

Nelle cartelle denominate "*BackupUtenti*", presenti sul desktop, ogni utilizzatore ha la possibilità di salvare periodicamente, sui dispositivi di rete, i propri file locali.

Su richiesta specifica del Dirigente responsabile, possono essere assegnate ai dipendenti *cartelle di procedimento* denominate con il procedimento cui fanno riferimento (es.: \\nas\Fascicolo elettronico).

Tutte le informazioni registrate nelle cartelle citate, sono quotidianamente salvate su un sistema di archiviazione, per garantire il loro puntuale ripristino in caso di eventuale corruzione e/o cancellazioni accidentali.

- d. Le cartelle predette sono aree di condivisione di 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 sulle quali vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale del settore SI.
- e. Non sono soggetti a salvataggio i dischi o altre unità di memorizzazione locali (es. disco C: e D: interni al PC).
- f. E' opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante. I files depositati nella cartella personale di backup non devono superare le dimensioni massime di 250 Mb;
- g. Non è consentita la memorizzazione di informazioni e/o documenti dell'Assessorato nei supporti di memoria esterni al DFS.



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

- h. Il personale del Settore SI può in qualunque momento procedere alla rimozione di file o applicazioni ritenuti pericolosi per la sicurezza sia dei PC sia delle unità di rete.

7.2. Antivirus

- a. Tutte le risorse della rete sono protette da un sistema antivirus centralizzato con strategie di protezione diversificate, relative alle attività periodiche di scansione, agli aggiornamenti dei motori di scansione e agli aggiornamenti quotidiani delle definizioni dei virus.
- b. Onde evitare la diffusione di eventuali virus tutti i supporti rimovibili, prima di essere utilizzati, devono essere sottoposti a scansione dal sistema antivirus.

7.3. Aggiornamento e distribuzione del software

- a. Gli aggiornamenti dei sistemi operativi avvengono con modalità totalmente automatica, attraverso appositi servizi telematici attivati dall'amministratore di sistema. L'allineamento dei software avverrà (in background) durante l'accensione e/o lo spegnimento della stazione di lavoro.

7.4. Internet

- a. Il PC assegnato al singolo utente con accesso a internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. Non è consentita, pertanto, la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
- b. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:
- l'upload o il download di software gratuiti (freeware e shareware), nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere contattato l'amministratore di sistema);
 - l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione generale (o eventualmente dal responsabile del Servizio di riferimento) e comunque nel rispetto delle normali procedure di acquisto;
 - ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
 - la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni i guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Dirigente responsabile.
- c. E' prevista l'adozione di uno specifico sistema di blocco o filtro automatico che impediscano determinate operazioni quali l'upload o l'accesso a siti inseriti in una black list.
- d. Le eventuali verifiche, compiute dall'amministratore di sistema, potranno avvenire mediante controllo dei contenuti (proxy server) o mediante la cronologia (file di log) della navigazione svolta. Il controllo sulla cronologia non è continuativo ed i file stessi vengono conservati non oltre 3 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza.



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

- e. Per evitare l'apertura di connessioni non filtrate è fatto divieto assoluto di utilizzo di apparecchiature modem per connessioni internet in ingresso od uscita.
- f. L'amministratore di sistema ha la facoltà di oscurare i siti e le pagine che difettino dei requisiti richiesti, o che siano in violazione di norme e regolamenti in vigore, o contenenti elementi di software che possano danneggiare i sistemi interni.

7.5. Posta elettronica

- a. La casella di posta elettronica istituzionale assegnata è uno strumento di lavoro. Gli assegnatari delle caselle sono responsabili del corretto utilizzo delle stesse.
- b. E' fatto divieto di utilizzare la propria casella di posta elettronica istituzionale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
 - l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
 - l'invio di allegati di dimensioni eccessive. Il servizio di posta elettronica della RAS è abilitato a contenere messaggi per massimo 100 MB;
 - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing – list;
 - la partecipazione a catene telematiche (o di Sant'Antonio). Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
 - l'invio in automatico di grandi quantità di mail (mail-bombing);
 - l'inoltro o la diffusione di messaggi pubblicitari ("Spam").
- c. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- d. È obbligatorio porre la massima attenzione nell'aprire i file allegati (attachments) di posta elettronica soprattutto se il mittente non è conosciuto o comunque non rappresenta una fonte attendibile².

² Gli allegati di posta elettronica sono una delle principali origini di infezioni da virus. È possibile ad esempio ricevere, anche da un mittente conosciuto, un messaggio di posta elettronica contenente un virus allegato sotto forma di documento, fotografia o programma. Se si apre il file, il virus infetterà il computer. Normalmente gli antivirus utilizzati sulla casella di posta istituzionale bloccano automaticamente i tipi di file pericolosi. Poiché tuttavia gli autori dei virus trovano spesso nuovi modi per diffondere malware, è sempre necessario prestare attenzione quando si apre un allegato. Se si ricevono allegati di posta elettronica di cui non si è informati, prima di aprirli, è consigliabile rispondere al mittente per verificare che li abbia effettivamente inviati. La stessa attenzione deve essere riposta per i collegamenti (link) contenuti nei messaggi. Quando si fa clic su un collegamento ingannevole è possibile visualizzare una pagina Web che cerca di scaricare malware sul proprio computer. Prestare attenzione quando si decide di fare clic su un collegamento in un messaggio, in particolare se il corpo del messaggio è vago e non specifico, ad esempio un messaggio con un testo come "Guarda le foto delle nostre vacanze" che non contiene informazioni personali che consentano di identificare il mittente e il destinatario.



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

CAPO III – ASSISTENZA E SERVIZI

ART. 8 - PROCEDURE OPERATIVE

- a. La richiesta per i seguenti servizi di assistenza dovrà essere inviata tramite il proprio Dirigente all'indirizzo mail admin.DGpers@regione.sardegna.it:
- sostituzione o attivazione di PC, stampante, scanner e altre apparecchiature;
 - creazione del profilo di posta elettronica e abilitazione all'accesso della casella di posta elettronica dell'ufficio;
 - accesso alle informazioni presenti nelle cartelle condivise;
 - creazione, modifica e cancellazione di un'utenza per l'accesso ai servizi della rete RAS;
 - prenotazione per il prestito di un PC portatile o di un apparato multimediale;
 - installazione di un nuovo applicativo;
 - abilitazione ai servizi erogati sulla Intranet;
 - abilitazione a servizi SAP SIBAR-HR.

In caso di impossibilità di erogare il servizio, ne sarà data motivata comunicazione al Dirigente richiedente e all'utente.

- b. In caso di ripristino del PC, stampante o altro dispositivo è sufficiente la richiesta direttamente da parte dell'utente.

CAPO IV – CONTROLLI E RESPONSABILITÀ

ART. 9 - CONTROLLI, RESPONSABILITÀ E SANZIONI

- a. La DG si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici, della posta elettronica e di internet, nel rispetto delle normative vigenti e in coerenza con quanto previsto dal presente regolamento.
- b. Per esigenze organizzative e di sicurezza, possono essere utilizzati strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, servizi o gruppi di utenti.
- c. Qualora – durante un controllo – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, l'Amministrazione procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento e alla normativa vigente, e si riserva la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
- d. La violazione da parte degli utenti dei principi e delle norme contenute nel presente regolamento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare.



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

ART. 10 - RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è autorizzato a:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete e degli applicativi, per copiare o rimuovere file e software;
- creare, rimuovere o resettare qualunque password previa comunicazione formale all'utente interessato delle motivazioni attinenti l'intervento;
- rimuovere programmi software, componenti hardware e dati non compatibili con quanto disposto dal presente regolamento;
- verificare l'eventuale esistenza di software non licenziato, operare per la sua rimozione immediata, informandone l'utente interessato ed il Direttore generale.

Le operazioni di cui sopra possono essere eseguite solo se rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

CAPO V – INFORMATIVA

ART. 11 - ENTRATA IN VIGORE DEL REGOLAMENTO

- a. Il presente regolamento entra in vigore il 01/07/2013. Dalla medesima data le disposizioni in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Sarà pubblicato su INTRAS, inviato alla casella istituzionale di ciascun dipendente e affisso nella bacheca della Direzione generale.
- b. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Le proposte verranno esaminate dalla Direzione generale.
- c. Il presente regolamento è soggetto a revisione con frequenza annuale.

Il Direttore Generale

Gesuina Tomainu



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

ALLEGATO A – MODULO DI PRESA VISIONE E ACCETTAZIONE DEL REGOLAMENTO

Il sottoscritto/a _____

matr. _____ assegnato al _____

Dichiara

- di aver preso visione ed accettare tutte le norme contenute nel regolamento d'uso del sistema informatico della Direzione generale;
- di aver acquisito le informazioni di cui all'art. 13 del D.lgs n. 196 del 30 giugno 2003 attinenti il "Codice in materia di protezione dei dati personali";
- di essere a conoscenza dei diritti dell'interessato di cui agli articoli 7, 8, 9, 10, 13 del medesimo decreto.

Data _____

Firma _____



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

D.Lgs 196/2003

Titolo II DIRITTI DELL'INTERESSATO

Art. 7

(Diritto di accesso ai dati personali ed altri diritti)

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
 - a) dell'origine dei dati personali;
 - b) delle finalità e modalità del trattamento;
 - c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
 - d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
 - e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
 - a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
 - b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
 - c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
 - a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
 - b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Art. 8

(Esercizio dei diritti)

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.
2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
 - a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
 - b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
 - c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
 - d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
 - e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
 - f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
 - g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
 - h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.
4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Art. 9

(Modalità di esercizio)

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10

(Riscontro all'interessato)

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
 - a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
 - b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.
2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.
4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.
5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.
7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

Art. 13 **(Informativa)**

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- e) i diritti di cui all'articolo 7;
- f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili e' indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

ALLEGATO B – GLOSSARIO

AMMINISTRATORE DI SISTEMA	Collaboratore cui è assegnato il compito di gestire il sistema informatico nella sua globalità e di assicurarne l'efficienza funzionale e i controlli di corretto utilizzo rispetto alle regole disposte dalla Direzione generale.
ANTIVIRUS	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che gli stessi virus hanno compiuto.
BACKUP	Copia di riserva di disco, di una parte del disco o di uno o più file.
BACKGROUND	(dall'inglese <i>background</i> che indica <i>sfondo</i> o <i>in secondo piano</i>) è una modalità di esecuzione tipica di alcuni programmi che non richiedono la presenza o l'intervento dell'utente, e che può essere concorrente all'esecuzione di altri programmi
BLACK LIST	Elenco di siti considerati non opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.
CHAT LINES	(in inglese, letteralmente, "chiacchierata"), viene usato per riferirsi a un'ampia gamma di servizi sia telefonici che via Internet
DATABASE	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
DFS	Archivio centrale condiviso della Direzione generale dove convergono i documenti generati dagli utenti
DOWNLOAD	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
DVD	Digital Versatile Disk (in italiano <i>Disco Versatile Digitale</i>) è un supporto di memorizzazione di tipo ottico.
E-MAIL	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica del computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
FILE ATTACHEMENT	File allegati alla e-mail che possono contenere virus
FILE DI LOG	Ha il significato di <i>giornale di bordo</i> , o semplicemente <i>giornale</i> , su cui vengono registrati gli eventi in ordine cronologico
FIREWALL	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
FREEWARE	Software gratuito realizzato e distribuito da privati o piccole società, attraverso internet o CD-ROM allegati a pubblicazioni in edicola.
FTP	File Transfer Protocol (<i>protocollo di trasferimento file</i>) è un protocollo per la trasmissione di dati tra computer.
GUESTBOOKS	(in inglese "libro degli ospiti") è un'utilità interattiva che permette ai visitatori di un sito web di poter lasciare firme e commenti.
HARD-DISK	Disco rigido del PC
HARDWARE	(letteralmente <i>ferramenta</i>) insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
HTTP	L'HyperText Transfer Protocol (protocollo di trasferimento di un ipertesto) è usato come principale sistema per la trasmissione d'informazioni sul web.
KNOW HOW	Identifica le conoscenze e le abilità operative necessarie per svolgere una determinata attività lavorativa
ICT	Information e communication technology (Tecnologie dell'informazione e della comunicazione)
INTERNET	Insieme mondiale delle reti di computer interconnesse.
INTRANET	Rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni
MAIL BOMBING	(letteralmente <i>bombardamento postale</i>) è una forma di attacco informatico in cui grandi quantitativi di e-mail vengono inviati ad un unico destinatario,



REGIONE AUTONOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA DE SA REGIONE
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE E RIFORMA DELLA REGIONE

Direzione generale dell'organizzazione e del personale

MALWARE	Indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito.
MP3	Tecnologia per la compressione/decompressione di file audio/video
NICKNAME (NICK)	Pseudonimo o "nome di battaglia", usato dagli utenti di Internet per identificarsi in un determinato contesto o in una determinata comunità virtuale.
PASSWORD	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito internet. E' necessario digitarla esattamente (caratteri maiuscoli/minuscoli), assieme alla user-id.
PROXY SERVER	E' un programma che si interpone tra un client ed un server facendo da tramite o interfaccia e filtro tra i due componenti ovvero inoltrando le richieste e le risposte dall'uno all'altro.
REMOTE BANKING	Servizi automatizzati che consentono ai clienti di collegarsi all'elaboratore della banca presso la quale intrattengono il rapporto di conto corrente tramite terminali interattivi trasportabili o installati nei propri locali
SAP	Piattaforma ERP sulla quale è stato sviluppato il sistema SIBAR.
SERVER	Indica genericamente un componente o sottosistema informatico di elaborazione che fornisce, a livello logico e a livello fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate <i>client</i> , cioè "cliente")
SHAREWARE	Software scaricabile via Internet ed utilizzabile in prova per un periodo variabile (30/60) giorni prima dell'acquisto.
Settore SI	Settore Sistema Informativo che, nell'ambito della Direzione, si occupa di impostare, indirizzare e coordinare l'introduzione delle tecnologie informatiche nell'attività della Direzione generale del Personale.
SOFTWARE	Programmi per i computer (professionali, ludici, video, musicali, raccolte di suoni ed immagini).
SPAM	Invio di messaggi indesiderati (generalmente commerciali).
SPYWARE	Tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.
SISTEMA INFORMATICO	Totalità dei PC, workstation, server, stampanti, apparecchiature di rete, strumenti hardware e software connessi alla rete informatica della Direzione generale.
USB	(Universal Serial Bus) è uno standard di comunicazione seriale che consente di collegare diverse periferiche a un computer.
USER ID	Nome utente
UTENTE (USER)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
VIRUS	Programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.
WORKSTATION	Stazione di lavoro, PC