ISPRA

Istituto Superiore per la Protezione e la Ricerca Ambientale

REGOLAMENTO ICT-ISPRA

Linee Guida per il Corretto Utilizzo delle Risorse Informatiche dell'ISPRA.
Misure per la prevenzione e il monitoraggio degli usi impropri.

Rev. 0 - gennaio 2013

INDICE

ART. 1 – FINALITÀ E PRINCIPI ISPIRATORI

Il presente Regolamento è finalizzato ai seguenti obiettivi:

- recepimento della Direttiva 02/09 della Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica
- recepimento della deliberazione del Garante per la protezione dei dati personali n.13 del 1 marzo 2007
- definizione delle corrette modalità di accesso ed uso delle Risorse ICT dell'Istituto.
- indicazione delle misure correntemente adottate per prevenire usi impropri di dette risorse e per monitorarne il corretto utilizzo in conformità al D.lgs. 196/2003 e s.m.i. (Codice della Privacy).

I suddetti obiettivi sono perseguiti assumendo come principi ispiratori:

- la massima sicurezza, protezione e integrità dei dati contestualmente alla loro corretta e adeguata disponibilità;
- la continuità operativa della strumentazione ICT stante la sua essenzialità per il funzionamento dell'Istituto.
- la minimizzazione dell'esposizione delle risorse ICT ad usi impropri e dannosi (anche inconsapevoli) sia dal punto di vista dell'economia complessiva dell'Istituto e sia dal punto di vista specifico della privacy.

ART. 2 – AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutti coloro che a qualsiasi titolo e in qualsiasi circostanza, sono formalmente autorizzati e abilitati all'uso delle risorse ICT dell'ISPRA.

ART. 3 – TUTELA DEL LAVORATORE

Nel rispetto dell'art. 4, comma 1, L. n. 300/1970, le misure adottate per prevenire gli usi impropri e per verificare il corretto utilizzo non prevedono in alcun modo l'installazione di "*apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*".

ART. 4 – MODALITA' DI ACCESSO ALLE RISORSE ICT

L'utente di norma accede alle Risorse ICT inserendo le proprie credenziali* (user-id* e password*) in un sistema che verifica l'identità e la sussistenza delle condizioni di abilitazione.
Le credenziali vengono fornite direttamente e in modo riservato dalla Struttura competente per la gestione dei sistemi informativi dell'Istituto.
In relazione alla necessità di contenere il numero di credenziali di accesso, nonché al fine di evitare l'uso improprio della rete informatica, ciascun responsabile di Dipartimento/Servizio e' tenuto a segnalare sollecitamente alla Struttura competente per la gestione dei sistemi informativi dell'ISPRA le utenze per le quali viene meno la necessità di accesso.
La Struttura competente per la gestione dei sistemi informativi dell'ISPRA procede in ogni caso, previa informativa al responsabile del Servizio, alla disattivazione delle credenziali di accesso alla rete e alla posta elettronica qualora non venga effettuato, per un periodo di 120 giorni consecutivi, alcun accesso. Da tale disattivazione sono esclusi i dipendenti di ruolo in posizione di comando presso altre PP.AA.

ART. 5 – MODALITA' DI UTILIZZO

Le Risorse ICT dell'ISPRA sono destinate ad attività di servizio ai fini dello svolgimento delle funzioni dell'Istituto, per la formazione del personale e per la gestione amministrativa.

E' vietata qualsiasi attività che possa produrre danni al funzionamento dell'Istituto o alla sua immagine o che risulti in contrasto con il dettato del presente disciplinare e/o con le leggi vigenti in materia.
Ogni utente è tenuto ad adottare comportamenti idonei a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi che abbiano come mezzo o fine le risorse informatiche.

ART. 5.1 CREDENZIALI DI AUTENTICAZIONE

Al primo accesso alle diverse risorse ICT l'utente procede alla modifica della password secondo le regole di composizione seguenti:

- deve essere alfanumerica e composta da almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Deve avere almeno un carattere alfabetico e almeno uno numerico, qualora si usi un solo carattere alfabetico o un solo carattere numerico questo non deve essere posto né ad inizio né alla fine della password;
- non deve essere composta da sequenze ascendenti o discendenti di cifre o lettere (per es. non si può usare "123456789" o "abcdefghi" o "ihgfedcba")
- non deve essere composta utilizzando la user-id;
- non deve essere ottenuta anagrammando la stessa password che deve essere cambiata
- deve rimanere segreta e l'utente deve custodirla con la massima diligenza in quanto è personalmente responsabile della eventuale cattiva custodia della stessa

La password deve essere cambiata con le stesse modalità ogni 6 mesi.

ART. 5.2 PERSONAL COMPUTER DESKTOP

Il Personal Computer affidato all'utente, che ne assume la responsabilità dell'utilizzo e cura ai sensi del presente regolamento, e' uno strumento di lavoro di esclusiva proprietà dell'ISPRA; pertanto il solo utilizzo autorizzato è quello inerente all'attività' lavorativa, ai sensi del vigente contratto di lavoro.
Di norma ogni utente è dotato di un unico personal computer ed è titolare di profilo di utilizzo* del tipo "power user*".
In caso di furto del PC o di sue component e accessori deve essere effettuata denuncia alla Pubblica Sicurezza; copia della denuncia deve essere fornita al Dipartimento Servizi Generali e Gestione del personale.
Non e' consentito riprodurre (in modo permanente o temporaneo, totale o parziale), tradurre, adattare, trasformare e distribuire software di proprietà di terzi, se espressamente vietato dalla licenza d'uso.
Non e' consentito all'utente modificare le impostazioni di sistema del proprio personal computer (PC).
E' consentito installare, con il supporto della struttura competente per la gestione dei sistemi informativi, programmi anche a titolo gratuito o periferiche hardware utili al lavoro, previa la verifica della loro compatibilità con il sistema in uso.
Non è consentito installare Software che non sia finalizzato allo svolgimento delle proprie attività di servizio.
E' consentito scaricare software via Internet solo se attinente alle proprie attività di servizio. E' responsabilità del singolo utente a cui e' assegnato il personal computer assicurarsi della disponibilità delle licenze dei programmi autonomamente installati.
La normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica dei programmi per elaboratore e L. 248/2000 nuove norme di tutela del diritto d'autore) impone la presenza nel sistema di software regolarmente dotato di licenza. L'inosservanza di questa disposizione, infatti, espone l'Istituto a gravi responsabilità civili e penali.

L’utente è tenuto a non fare copie di software, applicazioni, librerie di supporto, documenti e quant'altro sia riferibile o faccia parte delle Risorse Tecnologiche ISPRA e sia tutelato da diritti d'autore o diritti connessi o sui cui terzi vantino diritti morali e patrimoniali (D.Lgs. n. 68/2003, Legge 22 Aprile 1941 n.633 e successive modificazioni), ove questa possibilità non sia prevista esplicitamente dalle licenze di uso (GNU General Public License, GNU Library General Public License, Artistic License, BSD e BSD-style, Creative Commons, etc.).
Il Responsabile del Servizio, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività d’Istituto, in assenza dell’utente ha in qualunque momento la facoltà previa acquisizione di formale autorizzazione dell’utente medesimo da trasmettere al gestore del servizio informatico, di accedere ai dati trattati ivi compresi gli archivi di posta elettronica. Dell’operazione è redatto apposito verbale firmato dal responsabile del servizio e dal gestore del sistema che ha compiuto l’accesso.
Non e' consentita la memorizzazione di documenti informatici di natura oltraggiosa e o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione ed appartenenza sindacale o politica.
Non e' consentito utilizzare strumenti Software e/o Hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
Non e' consentito scaricare sulla propria postazione o sui server in rete file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria attività lavorativa.
L'accesso ai PC e' protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Nel caso in cui si lascia la postazione, anche se per breve tempo, il Personal Computer deve essere spento o reso inaccessibile tramite screen saver protetto da password.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore di sistema nel caso in cui vengano rilevati virus.
A meno di eccezioni concordate con i responsabili di struttura, tutti i personal computer, presenti presso gli uffici al termine della giornata lavorativa dovranno essere spenti ma non disconnessi dalla rete elettrica.

ART. 5.3 PERSONAL COMPUTER PORTATILE

I PC portatili vengono assegnati secondo una procedura interna pubblicata su Intranet.
L'utente è responsabile del PC portatile assegnato e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo.
In caso di viaggi il PC deve essere sempre trasportato come bagaglio a mano e sistemato in una custodia adeguata.
Ai PC portatili si applicano le regole di utilizzo in genere previste per i PC desktop connessi in rete fatta eccezione per i profili di accesso che nella fattispecie sono di tipo “administrator”.
All’atto della riconsegna del PC alla Struttura competente per la gestione dei sistemi informativi, particolare attenzione deve essere posta alla rimozione dei file di dati registrati sullo stesso, che in ogni caso saranno rimossi dal servizio informatico.
In caso di furto o smarrimento deve essere effettuata denuncia alla Pubblica Sicurezza; copia della denuncia deve essere fornita al Dipartimento Servizi Generali e Gestione del personale.
In caso di sottrazione, smarrimento o danno irreversibile al personal computer portatile l’utente è tenuto ad inoltrare alla Struttura competente per la gestione dei sistemi informativi dell’ISPRA nonché al responsabile del Dipartimento/Servizio di assegnazione un dettagliato rapporto che evidenzi, tra l’altro, le misure di custodia adottate.
Nel caso in cui sul PC portatile fossero presenti dati sensibili e/o giudiziari è opportuno richiedere agli amministratori di sistema l’installazione di un software di cifratura dei dati.
L’assegnatario in uso permanente deve periodicamente verificare la presenza e l’aggiornamento dell’antivirus segnalando eventuali inconvenienti alla Struttura competente per la gestione dei sistemi informativi dell’ISPRA.

ART. 5.4 RESTITUZIONE DELLE APPARECCHIATURE DI OFFICE AUTOMATION

Le apparecchiature di Office Automation (O.A.) in dotazione alle postazioni di lavoro sono di norma assegnate all'utente che ne possiede le credenziali di accesso. Allorché l'utente cessa di utilizzare detta strumentazione a causa di interruzione del rapporto con l'Istituto, o a causa di trasferimento ad altro Ente, le apparecchiature di O.A. devono essere restituite alla Struttura competente per la gestione dei sistemi informativi dell'ISPRA al fine di garantire la privacy e per favorire il più proficuo riutilizzo.

In particolare il Responsabile della Unità Organizzativa di secondo livello (UO) di appartenenza è tenuto ad inviare una comunicazione interna alla Struttura competente per la gestione dei sistemi informativi incaricata per il ritiro con la quale:

- informa della interruzione del rapporto dell'assegnatario con l'Istituto;
- segnala se il computer in questione contiene informazioni inerenti e utili alla propria attività di servizio indicando, nel caso, la necessità di preservare i relativi dati;
- dichiara, nel caso opposto, il proprio consenso alla cancellazione dei dati.

ART. 5.5 RETE TELEMATICA ISPRA

Per Rete telematica si intende un sistema di comunicazione che permette l'interconnessione delle strutture telefoniche ed informatiche, dette anche unità di rete, che servono diverse classi di utenti distribuiti su un'area più o meno ampia.

Le unità di rete contengono, in varia forma e su vari supporti, informazioni strettamente professionali che non possono in alcun modo essere utilizzate per scopi non professionali.

La responsabilità per il contenuto dei materiali diffusi attraverso la rete è delle persone che li diffondono.

L'utilizzo della rete per scopi personali è consentito per il tempo strettamente necessario all'assolvimento di incombenze amministrative/ burocratiche; in particolare si fa riferimento agli adempimenti on line nei confronti di pubbliche amministrazioni o concessionari di pubblici servizi, nonché di rapporti con istituti bancari ed assicurativi, ferma restando la possibilità di utilizzare la rete per finalità professionali o di organizzazione del lavoro anche in senso lato.

In merito all'utilizzazione delle unità di rete dell'ISPRA è vietato;

- entrare nella rete e nei programmi con altri nomi utente;
- danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password) e chiavi crittografiche riservate;
- inserire qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo religioso.

Nell'utilizzare la rete Telematica è inoltre vietato:

- collegare autonomamente tramite hardware (modem, router) la rete telematica ISPRA ad altre reti telematiche;
- collegare autonomamente tramite cavo, alla rete dati ISPRA apparecchiature per accessi wireless per non fornire anche involontariamente accesso dall'esterno alla rete telematica dell'Istituto;
- utilizzare hardware/software tali da consentire il controllo dei dati;
- collegare alla rete telematica ISPRA sottoreti impermeabili al monitoraggio operativo e funzionale della Struttura competente per la gestione dei sistemi informativi;
- svolgere sulla rete ogni altra attività vietata dalle leggi dello Stato, dalla normativa Internazionale, nonché dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle

reti e dei servizi di rete oggetto di accesso.
In relazione all'utilizzo delle stampanti è cura dell'utente ritirare prontamente le proprie stampe dai vassoi delle stampanti comuni.

ART. 5.6 POSTA ELETTRONICA

Per espletare le attività connesse ai compiti attribuiti all'Istituto deve essere utilizzata esclusivamente la casella di posta elettronica istituzionale. Detta casella può essere altresì utilizzata per altre comunicazioni, sempre che non ingeneri confusione nell'attribuzione all'Istituto dei contenuti del messaggio.
La casella di posta deve essere mantenuta in ordine, cancellando documenti ritenuti inutili, soprattutto se ingombranti.
La documentazione elettronica che costituisce per l'Istituto know how tecnico/scientifico o commerciale protetto sulla base della normativa vigente, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto non può essere comunicata all'esterno senza preventiva autorizzazione del proprio Responsabile.
Si devono controllare i file allegati ai messaggi di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
Non è consentito memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica
In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non sia possibile attivare la funzione autoreply o l'inoltro automatico su altre caselle aziendali, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al titolare della casella quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile.
A meno di non essere esplicitamente autorizzati dal destinatario è fatto assoluto divieto di leggere o rispondere a posta indirizzata ad altri.
Il proprio indirizzo di posta elettronica non può essere usato per l'invio di messaggi in nome e per conto di altri soggetti (ad esempio: associazioni, oo. ss., partiti politici),
La casella di posta elettronica è di norma disattivata all'atto della cessazione del rapporto dell'utente con ISPRA. Per specifiche esigenze di servizio è possibile prorogare fino a due mesi i termini per la disattivazione sulla base di una esplicita richiesta del responsabile alla struttura informatica competente.
Al fine di contrastare il fenomeno dello spamming (ricezione di posta indesiderata) devono essere seguite le seguenti regole:

- utilizzare i filtri per eliminare la posta indesiderata;
- non rispondere mai alle e-mail degli spammer, nemmeno per rimuovere il proprio nominativo dalla lista;
- mantenere disattivata l'anteprima nel programma di posta elettronica.

L'ISPRA provvede ad assegnare a tutti gli utenti dipendenti e comandati in entrata una casella di posta di tipo istituzionale nome.cognome@isprambiente.it. Vengono altresì generate, se richieste dal Responsabile della U.O. caselle di posta elettronica impersonali collegate a specifiche attività e comunque al progetto di riferimento.

ART. 5.7 INTERNET

L'accesso ad Internet è abilitato su tutti i personal computer connessi alla rete telematica.
Internet, fatto salvo quanto affermato all'art. 5.5, è di norma utilizzabile esclusivamente per finalità di servizio.
Non è consentito in particolare:

- l'utilizzo della navigazione in internet per scopi personali, fatti salvi i casi espressamente

previsti nel presente disciplinare;

- il caricamento o scaricamento di software gratuiti e shareware se non funzionali all'attività lavorativa;
- l'utilizzo di documenti provenienti da siti web se non funzionali all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione, (avvalendosi nel caso del supporto della Struttura competente per la gestione dei sistemi informativi dell'ISPRA);
- la registrazione a siti non correlati all'attività lavorativa;
- svolgere attività tendenti alla violazione del diritto d'autore o di altri diritti di proprietà intellettuale, o alla lesione di altre posizioni giuridiche soggettive tutelate dall'ordinamento;
- utilizzare internet provider diversi da quello ufficiale dell'ISPRA e connettere la postazione di lavoro alle reti di tali provider con sistemi diversi da quello centralizzato.

L'utilizzo della rete per scopi personali è consentito per il tempo strettamente necessario all'assolvimento di incombenze amministrative/ burocratiche; in particolare si fa riferimento agli adempimenti on line nei confronti di pubbliche amministrazioni o concessionari di pubblici servizi, nonché di rapporti con istituti bancari ed assicurativi.

Eventuali interruzioni del servizio di connessione alla rete Internet sono comunicate agli utenti con avvisi interni a cura della Struttura competente per la gestione dei sistemi informativi.

ART. 5.8 SUPPORTI RIMOVIBILI

Tutti i supporti rimovibili e riutilizzabili se contengono dati sensibili devono rispettare le cautele definite per i sistemi.
Ciascun utente è responsabile della custodia dei supporti e dei dati in essi contenuti.
I supporti magnetici contenenti dati personali o informazioni rilevanti per l'amministrazione devono in particolare:

- essere adeguatamente custoditi,
- essere utilizzati con particolare cautela al fine di evitare che il loro contenuto sia trafugato, alterato, distrutto o recuperato successivamente alla cancellazione;
- essere riutilizzati solo dopo aver eliminato i dati contenuti.

Al fine di assicurare la distruzione o l'inutilizzabilità di supporti magnetici rimovibili contenenti dati personali non più necessari per l'attività lavorativa, ciascun utente è tenuto a contattare il personale della Struttura competente per la gestione dei sistemi informativi dell'ISPRA e a seguire le istruzioni impartite allo scopo.

ART. 5.9 PROTEZIONE ANTIVIRUS

Il sistema informatico dell'ISPRA è protetto da software antivirus aggiornato quotidianamente.
Ciascun utente è comunque tenuto ad un comportamento tale da ridurre o, quantomeno, da non aggravare il rischio di attacco al sistema informatico mediante virus o altro software aggressivo.
Nel caso in cui il software antivirus rilevi la presenza di un virus non eliminabile, l'utente è tenuto a sospendere immediatamente ogni elaborazione in corso senza spegnere il computer, segnalando la circostanza al personale della Struttura competente per la gestione dei sistemi informativi dell'ISPRA.
Il software antivirus in uso verifica, inoltre, automaticamente ogni dispositivo rimovibile. Nel caso in cui sia rilevato un virus, l'utente è tenuto a mettere il dispositivo a disposizione del personale della Struttura competente per la gestione dei sistemi informativi dell'ISPRA per le necessarie verifiche.

ART. 6 - TRATTAMENTO DATI E CONTROLLI

ART. 6.1 CARATTERIZZAZIONE GENERALE

In ottemperanza a quanto stabilito dall'art. 4 del d.lgs. 300/1970, non vengono nel modo più assoluto utilizzate apparecchiature/strumentazioni hardware e software al fine di consentire controlli a distanza, prolungati, costanti o indiscriminati dei lavoratori.
È quindi nel pieno rispetto dei principi di pertinenza e di non eccedenza ed evitando ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, che l'Istituto si riserva di effettuare controlli sull'uso degli strumenti ICT.
Detti controlli sono svolti esclusivamente dalla Struttura competente per la gestione dei sistemi informativi.
I controlli effettuati di routine sono indiretti e di tipo aggregato. In particolare detti controlli sono finalizzati a verificare la funzionalità e la sicurezza dei sistemi.
Controlli indiretti di tipo aggregato, ma più specifici, vengono altresì attivati in caso di rilevamento di anomalie nell'utilizzo delle apparecchiature ICT.
Qualora la anomalia dovesse ripetersi e riguardare lo stesso ambito lavorativo si procederà con l'effettuazione di controlli più puntuali e su base individuale secondo le modalità di seguito indicate.

ART. 6.2 CONTROLLI SUI PERSONAL COMPUTER DESKTOP

La Struttura competente per la gestione dei sistemi informativi è autorizzata, previa comunicazione e contestuale accettazione dell'intervento da parte dell'utente interessato, a collegarsi in modalità remota ai PC delle singole postazioni di lavoro al solo fine di garantire l'assistenza tecnica e la normale attività manutenzione evolutiva nonché la massima sicurezza del sistema.
In particolare vengono tassativamente escluse:

- la lettura e la registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
- l'analisi occulta dei personal computer portatili affidati in uso.

L'accesso alle singole postazioni, è autorizzato in via eccezionale, allorché ricorra almeno una delle seguenti ipotesi:

- necessità di aderire a specifiche richieste di informazioni dell'Autorità giudiziaria;
- motivata richiesta dell'utente assegnatario della postazione di lavoro e titolare delle credenziali di autenticazione per l'accesso alla rete informatica dell'ISPRA;
- necessità dell'amministrazione connesse a particolari, specifiche e motivate esigenze di sicurezza.

ART. 6.3 CONTROLLI SULL'USO INTERNET E POSTA ELETTRONICA

In ottemperanza alla normativa vigente vengono tassativamente escluse:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esterni al di là di quanto tecnicamente necessario per la sola fornitura del servizio;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web dei siti visualizzati dall'utente;

I controlli sull'uso di internet e posta elettronica sono prioritariamente di tipo aggregato, riferiti all'intera struttura organizzativa dell'ISPRA o a sue aree. Detti controlli mirano a verificare esclusivamente l'accettabilità dei livelli di servizio disponibili e non evidenziano l'attività di una singola apparecchiatura, ovvero del singolo utente.
Qualora si riscontri un'anomalia che pregiudica la perfomance dei sistemi o la loro sicurezza, oppure giunga da parte dell'internet provider comunicazione di un non corretto comportamento di elaboratori in rete internet, vengono inviati avvisi agli utenti che, volontariamente o involontariamente, hanno causato tale comportamento

Detti avvisi evidenziando l'irregolare comportamento invitano gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
In caso di anomalie di funzionamento dovute a virus, viene attivata all'interno della Struttura competente per la gestione dei sistemi informativi una specifica procedura per la sua rimozione, eventualmente disabilitando l'utilizzo della rete dati o di applicazioni telematiche fino al ripristino dell'apparecchiatura che ha generato l'anomalia.
Sono comunque esclusi controlli prolungati, costanti o indiscriminati.

ART. 7 - SANZIONI

Preso atto che in base alle norme vigenti:

- ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche a cui ha accesso e dei dati trattati;
- ogni utente è responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene alla riservatezza dei dati ivi contenuti e la cui diffusione impropria potrebbe configurare violazione del segreto di ufficio o della normativa per la tutela dei dati personali;

sono vietati comportamenti che possano creare danno all'immagine dell'Istituto.

La violazione delle regole di cui al presente atto sarà valutata ai fini disciplinari e, ove ne ricorrano i presupposti, potrà comportare la denuncia dei trasgressori alle autorità competenti.

Nel caso in cui risulti necessario accertare eventuali ipotesi di responsabilità potrà essere disposta, previa comunicazione all'interessato, la revoca della possibilità di utilizzare in tutto o in parte le risorse informatiche dell'Istituto.

In particolare detta revoca si attua:

- se vi siano ragionevoli evidenze di uso non corretto del servizio da parte dell'utente;
- se vi siano ragionevoli evidenze di modifiche o interventi tecnici non autorizzati sull'hardware o sul software impiegati dall'utente per la connessione alla rete Internet;
- se vi siano ragionevoli evidenze che l'utente abbia reso disponibili a terzi parole chiave, procedure di connessione, indirizzo IP, credenziali di accesso a servizi telematici di carattere istituzionale o di servizio e altre informazioni tecniche da considerarsi riservate;
- se vi siano ragionevoli evidenze che l'attività dell'utente possa comportare danno, anche potenziale, al sito contattato;
- se l'utente abbia consentito l'accesso ad Internet a terzi per il tramite del proprio personal computer o utilizzando le proprie credenziali di autenticazione;
- in ogni altro caso in cui sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente circa il regolare utilizzo degli strumenti di servizio.

ART. 8 - PUBBLICITÀ ED ENTRATA IN VIGORE

Il presente Regolamento viene reso pubblico mediante:

- pubblicazione nell'albo web;
- comunicazione a tutti i titolari di casella di posta elettronica istituzionale dell'avvenuta pubblicazione nell'albo web;
- pubblicazione sul sito intranet dell'Istituto.

Il presente Regolamento entra in vigore il giorno lavorativo successivo alla data di pubblicazione sull'albo web

ART. 9 - TERMINI E DEFINIZIONI

Autenticazione	Azione di verificare l'identità di un utente e il fatto che egli abbia la prerogativa di poter accedere ad informazioni computerizzate. Progettato per proteggere da

	tentativi di collegamento illecito. L'autenticazione può anche riferirsi alla verifica di correttezza di un insieme di dati
Controllo accessi	Funzioni di sicurezza che hanno lo scopo di controllare che un utente possa espletare le sole operazioni di propria competenza.
Credenziale	Informazione conosciuta o posseduta unicamente da colui che ne è intestatario.
Dati sensibili	Ai sensi del Decreto Legislativo 196/03, dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o d'altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
Dati personali	Ai sensi del Decreto Legislativo 196/03, qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero d'identificazione personale così modificato dalla lettera *a*) del comma 2 dell'*art. 40, D.L. 6 dicembre 2011, n. 201*
Dato	Rappresentazione oggettiva di un fatto o evento tale da permetterne la sua trasmissione oppure interpretazione da parte di un soggetto umano o uno strumento informatico
Diritti di accesso	Detti anche "Permessi" o "Privilegi". Sono i poteri concessi agli utenti dall'amministratore o dal supervisore. I diritti di accesso determinano quali tipi di azioni l'utente può intraprendere – ad esempio lettura, registrazione, esecuzione, creazione, cancellazione – su archivi in volumi condivisi o su file server
ICT	Information &Communication Technology
Identificazione	Processo secondo il quale un utente dichiara la propria identità
Password	Stringa di caratteri protetta, generalmente cifrata dall'elaboratore, che autentica un categoria di utenti utente del sistema computerizzato
Power user	Nella terminologia Microsoft Windows indica una categoria di utenza caratterizzata da specifiche modalità/poteri di accesso e utilizzo della risorsa ICT.
Profilo (di utilizzo)	Termine generale usato per categorizzare le diverse modalità/poteri di accesso e utilizzo della risorsa ICT e in questo senso viene univocamente assegnato a ciascun utente (p. e. power user, administrator)
Trattamento dei dati personali	Ai sensi dell'art. 4 del D.Lgs. 196/03, "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il

	raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"
User ID	Identificativo dell'utente che abbinato alla password compone le credenziali dell'utente
Utente	"qualsiasi soggetto abilitato all'utilizzo dei servizi informatici dell'ISPRA, a prescindere dalla qualificazione giuridica e durata del suo rapporto con l'Istituto"

ART. 10 - NORME TRANSITORIE

Entro un anno dall'entrata in vigore del presente regolamento l'account di posta elettronica *nome.cognome@isprambiente.it* attualmente assegnato a personale che non sia dipendente né comandato in entrata, sarà modificato secondo le procedure ivi previste all'art. 5 "modalità di utilizzo", paragrafo "*Art.* 5.6 Posta elettronica".