REGOLE DI COMPORTAMENTO PER L'UTILIZZO DELLA POSTA ELETTRONICA E DEI SERVIZI DI RETE INTERNET

(Determina del Direttore Generale n. 19 del 23.02.2011, Allegato 1)

1. Organizzazione dei Servizi informativi della Sede centrale e delle Strutture di ricerca
   - Presso la Sede centrale e presso ciascuna Struttura di ricerca viene individuato, con determina rispettivamente del Direttore generale e del Direttore della Struttura, un dipendente quale Referente della Direzione per la gestione della rete locale (LAN) o, in caso di diversa configurazione, della gestione e della vigilanza delle infrastrutture informatiche.
   - Qualora al Referente siano affidate le funzioni di "Preposto agli adempimenti di natura informatica" ai sensi del decreto legislativo 30 giugno 2003, n. 196, egli viene nominato nei modi previsti dall'art. 8 del Regolamento per il trattamento dei dati personali del CRA e delle strutture afferenti;
   - Il Referente per la gestione della rete sarà scelto tra il personale di ruolo e individuato tra persone di adeguata competenza. Più strutture di ricerca possono, con l'accordo dei rispettivi Direttori, individuare una stessa persona come Referente per la gestione della rete. Nel caso l'amministrazione della rete sia affidata ad una Ditta esterna, le responsabilità del Referente per la gestione della rete ai fini del presente regolamento saranno affidate alla persona incaricata di tenere le relazioni con tale Ditta e di trasmetterle disposizioni riguardo alle regole da osservare.
   - Il nominativo del Referente per la gestione della rete deve essere comunicato al Servizio dell'Amministrazione centrale del CRA competente in tema di gestione del sistema informativo.
   - Ai fini del presente regolamento il Referente per la gestione della rete è la persona incaricata di verificarne l'attuazione, di impostare i controlli preventivi e successivi legittimi, di verificare l'esistenza e l'efficacia dei sistemi di protezione della rete locale da intrusioni ed abusi, di curare la consegna del materiale *hardware* e *software* al personale, controllare l'integrità dello stesso alla restituzione, informare gli utenti sulle modalità di loro uso corretto evidenziando potenziali rischi informatici e responsabilità degli utenti.
   - Il Referente per la gestione della rete è tenuto a limitare il proprio accesso alle informazioni di carattere privato al minimo necessario per assicurare l'integrità e la funzionalità dei sistemi ed è tenuto in ogni caso ad osservare l'obbligo del segreto professionale circa ogni informazione personale di cui venga a conoscenza in ragione della sua funzione.
2. Casella di posta elettronica individuale
   - Ad ogni lavoratore viene aperta una casella di posta individuale (*account*) nel dominio @entecra.it indipendentemente dalla funzione e dal tipo di rapporto di lavoro. Per l'attivazione deve essere compilato da

parte del lavoratore un modulo di richiesta disponibile sul sito web dell'Ente. L'Utente è responsabile dell'attività espletata tramite il suo *account* e pertanto è unico responsabile verso il CRA e verso terzi dell'uso delle proprie credenziali di accesso (nome utente e *password*). La casella *e-mail* personale non può essere aperta da altre persone se non nei casi previsti dalla legge e dal presente regolamento.

- Per i dipendenti con rapporto di lavoro a tempo determinato la casella di posta viene aperta su richiesta dell'interessato, utilizzando un modulo di richiesta disponibile sul sito web dell'Ente, tramite la Struttura presso la quale opera oppure dal Servizio. Deve essere individuata con certezza la data di conclusione del rapporto di lavoro.
- Previa comunicazione della Direzione Generale al competente Servizio, vengono attivate caselle di posta nominative per il Presidente, i Membri del Consiglio di Amministrazione, i Membri del collegio dei Revisori dei Conti, i Membri del Consiglio dei Dipartimenti, i Membri del Comitato di valutazione e i Membri dell'Organismo Indipendente di Valutazione.
- Caselle di posta individuali possono essere aperte, in casi particolari, previa approvazione del Direttore Generale, anche per persone estranee al CRA, quali esperti di altre Amministrazioni o ricercatori di altri Enti temporaneamente operanti presso il CRA.
- La casella di posta individuale viene chiusa dal competente Servizio dell'Amministrazione centrale non prima di un mese successivo alla cessazione del rapporto di lavoro o della funzione (per gli Organi) o della ragione per l'attivazione della casella (esperti o ricercatori esterni) e comunque non prima di un mese dall'invio all'interessato di un messaggio di preavviso della prossima chiusura. Deve essere cura dell'interessato garantire che le informazioni necessarie per lo svolgimento delle attività dell'Ente siano adeguatamente trasferite in modo da assicurare la continuità del servizio. La revoca dell'*account* comporta la cancellazione dei dati.
- Nelle comunicazioni via posta elettronica con il personale, l'Ente utilizza esclusivamente l'indirizzo di posta del dominio @entecra.it.
- Per coloro che non dispongano di una postazione individuale connessa ad Internet dovrà essere messa a disposizione una postazione libera nella quale, definendo modalità e orari di accesso compatibili con le esigenze del lavoro, sia consentito l'accesso alla posta elettronica.
- La casella di posta è uno strumento di lavoro e come tale deve essere utilizzata; i messaggi devono riportare in calce la "firma" che indichi quantomeno nome e cognome del mittente, la struttura di appartenenza, il suo indirizzo postale, il numero di telefono e di fax.
- In calce ad ogni messaggio deve essere riportata inoltre la seguente frase in lingua italiana e inglese (da inserire, possibilmente, nella "firma" dei messaggi):

  AVVERTENZE AI SENSI DEL DLGS 196/2003:

  Le informazioni contenute in questo messaggio di posta elettronica e/o nel/i file/s allegato/i, sono da considerarsi strettamente riservate. Il loro utilizzo è consentito esclusivamente al

destinatario del messaggio, per le finalità indicate nel messaggio stesso. Qualora riceveste questo messaggio senza esserne il destinatario, Vi preghiamo cortesemente di darcene notizia via e-mail e di procedere alla distruzione del messaggio stesso, cancellandolo dal Vostro sistema; costituisce comportamento contrario ai principi dettati dal Dlgs. 196/2003 il trattenere il messaggio stesso, divulgarlo anche in parte, distribuirlo ad altri soggetti, copiarlo, od utilizzarlo per finalità diverse.

PRIVACY DISCLAIMER:

Unless otherwise expressly stated, the information contained in this email is highly confidential and is intended only for the attention or use of the recipient named above. If you are not the intended recipient please inform the sender as soon as possible by email and delete the email and any attachment from your system. Any use, disclosure or copying of the present e-mail other than as authorized by us is prohibited.

- Il lavoratore deve essere consapevole che, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica istituzionale, i propri messaggi vengono ricevuti, acquisiti e trattati quale espressione della propria struttura lavorativa.
- Il Referente per la gestione della rete è autorizzato e tenuto ad attivare idonei sistemi di prevenzione dei rischi di intrusioni nei sistemi informatici e di ricezione di elementi nocivi (*malware*) quali virus, *worm*, *spyware*, *rootkit*, ecc. anche se questi sistemi bloccano messaggi di posta elettronica in arrivo o in partenza o i relativi allegati. Il blocco automatico dei messaggi da parte dei sistemi di protezione non costituisce violazione della sfera privata purché il contenuto dei messaggi non venga letto o diffuso o comunque utilizzato al di là delle strette necessità della sicurezza dei sistemi.
- Allo scopo di assicurare la continuità lavorativa, ogni dipendente che si assenti dal posto di lavoro per più di un giorno senza avere la possibilità di verificare la posta elettronica da altra postazione, deve inserire un messaggio di risposta automatica che avvisi dell'assenza e se necessario indirizzi i mittenti verso un altro collega o un ufficio.
- In caso di assenza non prevedibile, ad esempio per malattia, qualora il dipendente non sia in grado di ricevere e inviare comunque messaggi di posta elettronica tramite l'*account e-mail* personale aperto nel dominio @entecra.it, un fiduciario che conosca la *password* di accesso del dipendente e da questi espressamente autorizzato, può, su richiesta del Dirigente del Servizio o del Direttore della struttura di afferenza del dipendente, accedere alla posta e, se necessario, scaricare o inoltrare ciò che sia strettamente inerente le finalità del lavoro. Delle operazioni fatte sulla casella del dipendente in sua assenza viene redatto verbale sottoscritto dal fiduciario e tale verbale deve essere consegnato in copia al dipendente al suo rientro in servizio.
- Nel caso in cui urgenti esigenze di servizio lo giustifichino, il Dirigente del Servizio o il Direttore della struttura possono inoltrare al Servizio competente dell'Amministrazione centrale richiesta scritta e motivata

con la quale, sotto la propria responsabilità, richiedono di procedere alla sostituzione delle credenziali di accesso con contestuale notifica scritta al dipendente interessato; al rientro dell'assenza, è facoltà del lavoratore ripristinare la precedente *password*, o sostituirla con altra personale.

3. Caselle di posta elettronica degli uffici
   - Per le esigenze dell'Amministrazione possono essere aperte nel dominio @entecra.it caselle di posta per Servizi, Uffici o altre unità organizzative dell'Amministrazione centrale o delle Strutture di ricerca con modalità definite nel disciplinare di cui al quarto comma del presente articolo. Per ogni casella viene individuato il responsabile della gestione delle credenziali di accesso.
   - Alle caselle di posta degli uffici devono poter accedere le persone individuate dal Dirigente responsabile del Servizio o dal Direttore della Struttura di afferenza.
   - Le caselle di posta degli uffici debbono essere lette con cadenza almeno giornaliera; durante i periodi di ferie dovrà essere assicurata comunque la lettura attraverso una turnazione del personale autorizzato alla lettura o la concessione temporanea dell'accesso a personale di altri uffici che possa far fronte alle incombenze ordinarie.
   - Con apposito disciplinare, da emanarsi con Determina del Direttore Generale entro sessanta giorni dall'approvazione del presente Regolamento, vengono definite le regole per un'omogenea denominazione delle caselle di posta elettronica degli uffici.
   - Il competente Servizio dell'Amministrazione centrale predispone liste di distribuzione per agevolare l'invio di comunicazioni via posta elettronica a specifici gruppi di destinatari. Messaggi indirizzati alle liste di distribuzione possono essere inviati solo dalle caselle istituzionali (Direzioni, Servizi, Uffici, Strutture di ricerca). Ogni invio da caselle di posta individuali sarà bloccato. L'impiego di alcune liste di distribuzione potrà essere riservato a determinate Direzioni, Servizi, Uffici.
4. Navigazione in Internet
   - La "navigazione" in Internet va limitata alle finalità del servizio, accedendo esclusivamente a siti pertinenti ai propri compiti istituzionali.
   - Non è consentito scaricare da Internet o scambiare file (es. immagini, musica, filmati o *software*) che non siano inerenti le attività di lavoro.
   - Nello scaricare *software* o altro materiale ancorché inerente le attività di lavoro va osservata ogni possibile precauzione per evitare l'importazione di virus o altri agenti dannosi. Prima di scaricare *software* il Dipendente si accerta della piena legalità del suo utilizzo. Non è consentito scaricare o installare *software* senza aver accertato ed accettato le condizioni del Contratto di licenza.
   - Non è consentito effettuare tentativi di intrusione su sistemi interni all'Ente o di altri soggetti pubblici o privati, anche se non protetti da adeguati sistemi di sicurezza; eventuali operazioni o transazioni finanziarie tramite Internet necessarie per lo svolgimento dell'attività

lavorativa (es. acquisto on-line di biglietti ferroviari o aerei) debbono essere eseguite nel rispetto delle normali procedure di acquisto.

- Non è consentito partecipare per motivi non professionali a Forum, *chat line*, bacheche elettroniche, registrazioni in *guestbook*, attivazione di servizi RSS, anche utilizzando pseudonimi.

5. Attività di prevenzione di abusi
   - Il Referente per la gestione della rete avrà facoltà di prevenire abusi nell'uso di Internet tramite accorgimenti nella configurazione dei *firewall* o delle singole postazioni di lavoro quali la chiusura di porte, l'introduzione di filtri che impediscano l'accesso a determinati siti o a determinati tipi di file.
   - La *black list* dei siti bloccati e i sistemi similari di protezione, possono essere aggiornati autonomamente dal Referente per la gestione della rete. Il competente Servizio dell'Amministrazione centrale potrà diramare direttive sulla composizione della *black list* e sulle modalità di attuazione dei blocchi cui gli Amministratori per la gestione della rete delle Strutture di ricerca dovranno conformarsi.
   - Potranno essere attivati sistemi di avviso automatico (es. con messaggi *pop up*) che segnalino al dipendente situazioni in cui egli stia attuando un comportamento non conforme al presente regolamento. Il destinatario del messaggio non deve essere registrato dal sistema.
   - Per le pagine *web* bloccate sarà cura del Referente per la gestione della rete fornire indicazioni circa le modalità necessarie per richiedere la rimozione del blocco.
6. Controlli
   - Controlli sull'osservanza delle norme di cui al presente regolamento sono demandati esclusivamente al Referente per la gestione della rete di cui all'articolo 1, salvo il caso in cui, per il sospetto di comportamenti illegali, sia intervenuta l'Autorità giudiziaria.
   - Controlli vietati. E' vietato, anche al Referente per la gestione della rete, leggere il contenuto dei messaggi di posta, registrare le pagine *web* visitate dal singolo lavoratore, usare *software* che consenta di ricostruire la sequenza di tasti premuti. Nel caso di accesso non intenzionale o per motivi legati alla sicurezza dei sistemi, egli è tenuto al segreto professionale e, se dei dati acquisiti debba essere data parziale diffusione (ad esempio a Ditte esterne incaricate di interventi per la manutenzione) deve avere cura di eliminare ogni riferimento che consenta il collegamento a soggetti interni o esterni all'Ente o affidare il computer a ditte specializzate che a loro volta garantiscano il segreto professionale.
   - Controlli ammessi. Sono ammessi, e periodicamente effettuati dal Referente per la gestione della rete, controlli collettivi (per Struttura, Servizio, Ufficio) che non consentano il riferimento a singoli individui. Potranno essere oggetto di controllo collettivo, tra l'altro, i tempi di collegamento a Internet, i siti visitati, i volumi di dati scambiati, i tipi di file scaricati o scambiati. Nel caso ravvisi situazioni anomale, il Referente per la gestione della rete ne dà comunicazione scritta, anche

in forma di messaggio di posta elettronica, al responsabile dell'unità controllata il quale è tenuto ad informarne il personale interessato.

- In caso di documentata persistenza di situazioni anomale, segnalate al personale secondo quanto previsto dal punto precedente, il Referente per la gestione della rete ne informa il Direttore della struttura o il Dirigente responsabile del Servizio.
- Ogni forma di controllo individuale con o senza la preventiva informazione dell'interessato può essere effettuata solo su disposizioni e sotto il controllo dell'Autorità giudiziaria.
- I "file di *log*" vengono archiviati per il tempo strettamente necessario alla sicurezza dei sistemi e alle esigenze di applicazione del Decreto legislativo 30 giugno 2003 , n.196, salvo esigenze straordinarie (ad es. in funzione di indagini giudiziarie).
- E' facoltà del Referente per la gestione della rete, dandone preavviso all'interessato, effettuare o far effettuare controlli sulle postazioni individuali finalizzati alla sicurezza dei sistemi informatici, quali il rilevamento e l'eliminazione di virus, l'installazione/disinstallazione di *hardware* o *software*, la verifica di malfunzionamenti. Tali operazioni, di norma, devono essere effettuate in presenza dell'interessato o di un suo fiduciario qualora si debbano utilizzare *password* di accesso o si debba accedere ad aree della memoria suscettibili di rivelare informazioni personali.

7. Sanzioni
   - La non osservanza delle norme di condotta di questo regolamento viene sanzionata secondo le normali procedure disciplinari. Ove siano rilevabili fatti che possano costituire illecito penale o violazione di leggi, l'Amministrazione segnalerà la circostanza all'Autorità giudiziaria.
8. Norme generali, transitorie e finali
   - Per quanto non previsto dal presente regolamento, valgono le norme generali dell'ordinamento italiano, in particolare quelle relative alla tutela della privacy, alla protezione dei dati e agli usi per finalità illegali degli strumenti telematici. Valgono inoltre le disposizioni di cui al Regolamento per il trattamento dei dati personali del CRA e delle strutture afferenti, Titolo 1 capo 1. e del D.Lgs. n. 82/2005 e successive modificazioni ed integrazioni "Codice dell'amministrazione digitale".
   - Il presente Regolamento potrà essere accompagnato o seguito da circolari esplicative emanate dall'Amministrazione che, pur nel rispetto dei principi generali, definiscano modalità di attuazione o norme tecniche ad esso correlate.