REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLA RETE INTERNET E DELLA POSTA ELETTRONICA

Sommario

1 PRINCIPI GENERALI

Il presente documento, in applicazione delle prescrizioni definite dal Codice di Comportamento Interno di Gruppo, ha l'obiettivo di regolamentare l'utilizzo di internet e posta elettronica per gli utenti di tali servizi.

Le presenti regole di sicurezza hanno valenza per la Banca si pongono l'obiettivo di fornire agli utenti idonee misure di sicurezza e linee di comportamento adeguate per utilizzare in modo conforme e non rischioso la posta elettronica aziendale e la navigazione in internet.

Le predette regole di sicurezza vengono ordinate in un unico Regolamento il quale armonizza e riunisce in un unico corpo normativo la disciplina esistente sul tema.

Il Regolamento è adottato in conformità al Provvedimento del Garante per la tutela dei dati personali del 1° marzo 2007 e le disposizioni in esso contenute attengono ad aree sensibili del Modello di organizzazione, gestione e controllo adottato ai sensi del D. Lgs. 8 giugno 2001, n. 231 e successive modificazioni e integrazioni.

A tal proposito, allo scopo di rappresentare agli utenti il quadro normativo di riferimento si specifica che le principali fonti normative in materia sono le seguenti:

- Decreto Legislativo n.196 del 30/06/2003 c.d. Codice della Privacy (di seguito "Codice");
- Provvedimento del "Garante della Privacy" n. 13 del 01/03/2007 (di seguito "Provvedimento");

Copia del regolamento viene pubblicata nella intranet aziendale nella sezione "Manuali" (Siti Intranet della Banca → Strumenti Operativi→ Documenti→ Normativi→ Manuali) e consegnata a ciascun dipendente all'atto dell'assunzione ed a ciascun collaboratore ad inizio attività.

Il Servizio Sicurezza è l'attuale Responsabile per l'Implementazione Normativa in materia di Privacy e può essere contattato scrivendo all'indirizzo di posta elettronica assistenzaprivacy@cariparma.it.

2 CAMPO DI APPLICAZIONE

Il presente Regolamento si applica:

- a tutti i lavoratori dipendenti e a tutti i collaboratori della Banca a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, *stagisti*, consulenti, ecc.) di seguito "utenti";
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

3 UTILIZZO DEGLI STRUMENTI INFORMATICI DI LAVORO

Per quanto riguarda l'accesso e l'utilizzo dei sistemi informativi e in generale di tutte le dotazioni correlate al posto di lavoro si rimanda alla circolare di riferimento "Sicurezza informatica - Regole di sicurezza dei sistemi informativi" (Circ. 2011/135).

Si riportano di seguito alcune prescrizioni di carattere generale:

- le dotazioni assegnate all'utente (ad es. postazioni di lavoro, pc portatili, palmari, blackberry, telefoni aziendali, ecc…) sono strumenti di lavoro che devono essere custoditi evitando danneggiamenti, sottrazioni, accessi / utilizzi non consentiti;
- è vietato l'utilizzo dei medesimi strumenti per finalità non attinenti l'attività lavorativa: per attività lavorativa si intende lo svolgimento della prestazione lavorativa assegnata e la gestione del rapporto di lavoro dell'utente dipendente (riguardante ad esempio il contratto di lavoro, la busta paga, la gestione delle trasferte, la previdenza complementare, il CRAL, la Cassa Mutua, ecc..), fermo restando che le comunicazioni relative a tali ultime finalità devono essere indirizzate solo a Strutture aziendali competenti oppure a strutture esterne autorizzate (es. Agenzia Viaggi per prenotazioni alberghiere e mezzi di trasporto in caso di trasferta);

- è consentito solo l'utilizzo dei programmi ufficialmente installati dal Personale aziendale (è vietato agli utenti installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dalla Banca);
- è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna);
- ogni utente deve prestare la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), avvertendo immediatamente il Personale incaricato del Servizio Sicurezza nel caso in cui siano rilevati virus.

Ogni finalità e ogni contenuto non conforme a quanto stabilito nel presente Regolamento è espressamente vietato.

4 POSTA ELETTRONICA AZIENDALE

L'utilizzo della posta elettronica è consentito a ciascun dipendente, nonché ai collaboratori esterni dotati di utenza e di abilitazione all'utilizzo dei sistemi informatici.

Le istruzioni operative per l'accesso e l'utilizzo della posta elettronica aziendale sono contenute nel Manuale Operativo al quale si rimanda (disponibile al seguente percorso: "Strumenti Operativi" – "Documenti" – "Normativi" – "Manuali" alla Materia-Parola chiave: Sistema Informativo- Internet/Posta Elettronica).

Ribadendo il principio che la casella di posta elettronica aziendale assegnata è uno strumento di lavoro e che pertanto deve essere utilizzata esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa, di seguito si prescrivono le norme di comportamento che devono essere adottate:

- è vietato l'utilizzo con contenuti e/o per finalità attinenti la sfera privata e personale dell'utente (sia la messaggistica diretta all'esterno dell'Azienda sia quella interna);
- è vietato l'utilizzo della casella di posta elettronica da parte di persone diverse dall'assegnatario.

Di seguito vengono descritte nel dettaglio le regole di fruizione e i comportamenti da seguire per l'assegnazione, l'utilizzo e la gestione della posta elettronica.

4.1 Assegnazione

Ad ogni utente viene assegnata una casella di posta aziendale nominativa, strumento che deve essere utilizzato esclusivamente per finalità connesse allo svolgimento dell'attività lavorativa.

L'assegnazione di un indirizzo di posta elettronica aziendale e la conseguente abilitazione all'utilizzo di tale servizio avviene:

- per l'utente interno, automaticamente al momento dell'inserimento del nominativo nel sistema informatico aziendale, da parte delle strutture competenti;
- per l'utente esterno, al momento della richiesta di attivazione da parte del Responsabile della struttura a cui l'utente esterno è assegnato.

Inoltre, per ogni Unità Organizzativa è operativa una corrispondente casella di struttura visionabile dal Responsabile dell'unità organizzativa, dal Vice (laddove presente) e da eventuali collaboratori delegati dal Responsabile.

Tutti i dipendenti sono invitati ad utilizzare le caselle d'ufficio, per ovviare alle problematiche derivanti da assenze improvvise, prolungate o comunque non programmate di cui al successivo parargafo, riservando l'uso delle caselle aziendali nominative alle comunicazioni strettamente interne o aventi carattere organizzativo (ad esempio, inviti a riunioni; inoltro mail per conoscenza etc.)

Sono previste altresì per esigenze operative delle caselle di reparto (posta specialistica) che vengono attivate su specifica richiesta del Responsabile della struttura organizzativa mediante invio del modulo elettronico 358.

4.2 Modifica o disattivazione del servizio

L'indirizzo di posta elettronica aziendale è legato all'abilitazione dell'utente nel sistema informatico aziendale pertanto, in caso di trasferimento del Personale fra strutture o modifiche del rapporto di lavoro, saranno applicate le seguenti disposizioni.

Per l'utente interno:

- in caso di trasferimento ad altra unità organizzativa (ad es. da Direzioni Centrali a Rete e viceversa), viene garantita la continuità ed il passaggio dei contenuti della posta, rispettando i limiti della dimensione della casella stabiliti per l'unità organizzativa di destinazione;
- in caso di distacco totale o parziale presso altra Società del Gruppo, viene attribuito un nuovo indirizzo di posta in funzione della nuova società di lavoro. L'utente potrà comunque continuare a ricevere ed avere visibilità della posta ricevuta al vecchio indirizzo potendo tuttavia scrivere solo con il nuovo indirizzo;
- in caso di cessione di contratto, l'utente non potrà più utilizzare o vedere il contenuto della posta del precedente indirizzo;
- in caso di cessazione del rapporto di lavoro, l'indirizzo di posta elettronica sarà disabilitato contestualmente alla disattivazione dell'utente.

Per l'utente esterno:
si provvederà alla disattivazione dell'utenza facendo riferimento alla data di scadenza indicata nella richiesta di attivazione.

4.3 Autenticazione dell'accesso alla casella

L'accesso alla casella di posta elettronica individuale non richiede l'inserimento della parola chiave (*password*), in quanto l'utente viene autenticato ed abilitato ad accedere alla posta al momento della digitazione della parola chiave prevista per il collegamento alla Rete Aziendale.

4.4 Assenza dal servizio

L'utente, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno una giornata lavorativa - deve attivare l'apposita funzionalità di sistema (cd. "Fuori Sede") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.

L'azienda, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo dell'Ufficio Sicurezza Logica, di accedere alla casella di posta elettronica dell'utente assente: per i dettagli si rimanda al paragrafo "Accesso ai dati dell'utente".

4.5 Firma nei messaggi di posta elettronica

I messaggi di posta elettronica inviati devono sempre riportare la firma dell'utente mittente. Tale firma deve essere redatta unicamente utilizzando gli standard di seguito riportati che prevedono anche l'inserimento di un'apposita dicitura ai sensi della normativa sulla Privacy (cd. *Disclaimer*): non sono pertanto ammesse firme personalizzate non conformi ai modelli di seguito descritti (ad. es. utilizzando i caratteri, colori e forme difformi dallo standard della Banca).

Al fine di evidenziare anche ai destinatari la natura esclusivamente aziendale della casella di posta elettronica, i messaggi in uscita devono contenere un avvertimento standardizzato *(Disclaimer)* nel quale viene dichiarata la natura non personale dei messaggi stessi.

Si coglie l'occasione per precisare che la firma di ogni e-mail deve essere obbligatoriamente provvista dell'indicazione del nome e cognome del dipendente che ne effettua l'invio, sia che l'e-mail venga inviata dalla casella nominativa attribuita al Dipendente o al collaboratore, sia che venga inviata da quella dell'ufficio/reparto di appartenenza.

Per ogni dettaglio ulteriore relativo alla firma ed al disclaimer si rinvia all'apposita sezione del Brand Book presente nel Portale di Gruppo (percorso: Portale di Gruppo Galileo → Comunicazione → Brand Book → Riferimenti in calce alla mail) e alla Circolare"Riferimenti in calce alle e-mail" di prossima emanazione.

4.6 Manutenzione: pulizia delle caselle

Al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere "tenuta in ordine" cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.

Il sistema di posta elettronica aziendale prevede un automatismo che consente lo svuotamento delle cartelle relative alla "Posta eliminata".

L'automatismo procede centralmente ad attivare una funzionalità di svuotamento automatico dei contenitori di "posta eliminata", presenti all'interno delle singole caselle (personali, di reparto, d'ufficio); tale automatismo opera dopo 10 giorni dall'eliminazione della e-mail dalla posta corrente.

I messaggi di posta elettronica eliminati vengono allocati temporaneamente (ulteriori 10 giorni) nella cartella "Recupero posta eliminata" nella quale sono disponibili per un eventuale ripristino prima della definitiva cancellazione.

4.7 Sistema Antispam

E' attivo un sistema antispam sulle mail in entrata ed in uscita provvedendo alla cancellazione delle mail che sono individuate come spam (per spam si intendono i messaggi di posta elettronica non inerenti l'attività lavorativa e non sollecitati da chi li riceve).

Le mail che vengono individuate e classificate dal sistema con una minore probabilità di essere spam sono, invece, temporaneamente archiviate nella cartella "Posta indesiderata".

Nel caso in cui l'utente reputi alcuni messaggi ricevuti nella cartella "posta in arrivo" come messaggi di spam deve spostarli nella cartella "Spam Mail".

Questi messaggi sono archiviati temporaneamente in tale cartella per un periodo di 60 giorni, al termine del quale vengono automaticamente eliminati.

L'utente è tenuto a:

- verificare giornalmente i messaggi pervenuti nella cartella "Posta indesiderata", evitando di rispondere al mittente;
- esaminare l'oggetto ed il testo dei messaggi pervenuti evitando di cliccare su "link" eventualmente presenti o di aprire gli allegati;
- inviare alla casella di ufficio CU862 il messaggio originale in allegato utilizzando l'apposita funzione "Inoltra come allegato" per segnalare messaggi aventi connotazione di "spam", in caso di fenomeno ripetitivo e persistente.

4.8 Cautele nella predisposizione dei messaggi

Nell'utilizzo della posta elettronica il Personale deve tenere in debito conto che i soggetti esterni attribuiscono carattere istituzionale alla corrispondenza ricevuta da dipendenti aziendali. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione della Banca.

A tal proposito, al fine di migliorare la qualità della comunicazione in entrata e in uscita, il servizio di Posta elettronica aziendale è dotato di una funzionalità che blocca l'invio o la ricezione di messaggi, qualora questi contengano vocaboli non in linea con la prassi aziendale. Si rinvia alla Lettera Circolare (2009/124) "Posta elettronica - Attivazione funzionalità di Content Filtering" per maggiori dettagli.

La Banca formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi.

a) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni contrattuali o precontrattuali per la Società;
b) prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi gli utenti devono in particolare:
   - visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,
   - una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti,
   - cancellare il messaggio e svuotare il "cestino" della posta,
   - segnalare l'accaduto all'Help Desk Tecnico;
c) evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;
d) in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica :
   - adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio; in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,
   - utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di *social engineering*,
   - in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa. Si raccomanda, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca.
e) in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;
f) evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

Inoltre, al fine di instaurare una corretta ed efficace comunicazione tramite posta elettronica, la Banca ha recentemente pubblicato un Manuale "Regole Base per un'email efficace" disponibile nel Portale di Gruppo nella sezione Comunicazione.

5 NAVIGAZIONE INTERNET

L'utilizzo di internet è consentito a ciascun dipendente, nonché ai collaboratori esterni dotati di utenza e di abilitazione all'utilizzo dei sistemi informatici.

Ribadendo il principio che il servizio Internet rilasciato dalla Banca è uno strumento di lavoro e che pertanto deve essere utilizzato esclusivamente per finalità strettamente connesse allo svolgimento dell'attività lavorativa, di seguito si prescrivono le norme di comportamento che devono essere adottate.

A titolo esemplificativo è vietato utilizzare Internet per:
- finalità ludiche o estranee all'attività lavorativa;
- l'upload o il download di software gratuiti (freeware) e shareware, a titolo di prova o protetti da copyright;
- scaricare programmi eseguibili o con estensione a rischio (es. .exe, .com, .ovr, .ovl, .sys, .vbs, .shs, .pif, .bat, ecc.), nonché utilizzare documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere contattata il competente Ufficio Sicurezza Logica inviando una mail alla casella di ufficio CU862);
- partecipare a forum non professionali, utilizzare chat-line, blog, bacheche elettroniche (esclusi gli strumenti autorizzati);
- effettuare la propria registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- inviare, in generale, informazioni non pubbliche della propria azienda, salvo specifica autorizzazione;
- accettare gli eventuali download di file non richiesti dall'utente durante l'accesso ad Internet.

E' fatto divieto inoltre di riutilizzare, nelle registrazioni a servizi Internet e su siti esterni di qualunque tipo, gli stessi codici (user-ID e/o password) utilizzati sui sistemi aziendali.

Al fine di mantenere costantemente efficienti e stabili i sistemi di trasmissione dati aziendali l'utente è tenuto ad utilizzare la navigazione internet nei siti autorizzati accedendo a contenuti strettamente attinenti all'attività lavorativa e con una durata di connessione che sia adeguata all'esecuzione dei compiti assegnati.

5.1 Abilitazione del servizio Internet e modalità di accesso

L'utente in possesso di credenziali di accesso è automaticamente abilitato ad accedere al servizio di navigazione internet.

L'accesso ad Internet avviene mediante il browser di navigazione Internet Explorer e non richiede l'inserimento di utenza e password in quanto l'autenticazione avviene automaticamente utilizzando le credenziali inserite in fase di accesso al Sistema Informatico.

5.2 Sospensione o disattivazione del servizio Internet

Il servizio internet viene automaticamente sospeso in caso di "lunga assenza" (es. lunghe malattie, aspettative, maternità, ecc). In caso di cessazione del rapporto di lavoro (es. dipendente, stagista) ovvero decorsi i termini contrattuali (es. collaboratore) l'utenza viene disabilitata e pertanto il servizio internet non è più fruibile.

5.3 Filtri

Al fine di ridurre il rischio di navigazione in siti non pertinenti l'attività lavorativa è stato previsto un sistema di filtraggio automatico riguardante l'accesso a siti Internet, l'upload (caricamento) ed il download (scaricamento) dei file dal web prevenendo determinate operazioni.

A tale scopo il Personale è stato suddiviso nei seguenti tre gruppi interni di appartenenza: Rete, Direzione Centrale e Abilitazioni straordinarie.

<u>Accesso ai siti Internet</u>
Il sistema suddivide automaticamente i siti Internet in categorie tematiche (es. Affari, Informazione, Trasporti, ecc..) associando tali categorie ai citati gruppi interni di appartenenza.
Il Personale è pertanto abilitato ad accedere unicamente ai siti consentiti dal proprio gruppo di appartenenza. Ne consegue che viene automaticamente bloccato l'accesso a siti appartenenti a categorie reputate incoerenti con la prestazione lavorativa: in tal caso il sistema propone un messaggio riportante la motivazione del blocco con l'evidenza della categoria associata.

<u>Upload e Download dei file</u>
Il sistema è configurato per verificare le caratteristiche di determinati file o software consentendo l'upload o il download in funzione del gruppo di appartenenza.
In caso di upload o download non autorizzato il sistema propone un messaggio riportante la motivazione del blocco.

Qualora l'utente entri accidentalmente in siti contrari ai principi contenuti nel Codice Etico di Gruppo è tenuto a terminare immediatamente il collegamento e a segnalare, tramite mail, l'anomalia all'Ufficio Sicurezza Logica affinché possa effettuare l'aggiornamento delle blacklist.

Nel caso si ravvisi la necessità di accedere, esclusivamente per ragioni lavorative, ad uno o più siti non consentiti dal proprio profilo di appartenenza si dovrà inviare apposita richiesta mediante il modulo elettronico 358. L'Ufficio Sicurezza Logica, valutata l'ammissibilità della richiesta pervenuta, provvede ad inserire i siti segnalati tra quelli consentiti.

Eventuali abilitazioni all'accesso illimitato, adeguatamente motivate, dovranno essere richieste tramite e-mail alla casella di ufficio CU862, previa esplicita approvazione da parte del Responsabile della struttura gerarchicamente superiore.

Al Personale esterno è data la facoltà di accedere alla rete Intranet aziendale mentre è bloccato l'accesso alla rete Internet ad esclusione dei link strettamente legati alle esigenze lavorative (previa richiesta di

autorizzazione da inviare a cura del Referente interno). Per il Personale in stage l'accesso sarà concesso soltanto dietro specifica richiesta del Responsabile dell'unità operativa dove opera lo *stagista*.

6 ACCESSO AI DATI DELL'UTENTE

Il personale incaricato dell'Ufficio Sicurezza Logica e del Servizio Infrastrutture può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.

Il personale incaricato dell'Ufficio Sicurezza Logica e del Servizio Infrastrutture può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).

Il personale incaricato dell'Ufficio Sicurezza Logica e del Servizio Infrastrutture può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

L'eventuale controllo sui file di log da parte del personale incaricato dell'Ufficio Sicurezza Logica e del Servizio Infrastrutture, non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

Il personale incaricato del Servizio Infrastrutture è abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.
Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.

In ogni caso, il Gruppo Cariparma Crédit Agricole garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

7 CONTROLLI GRADUALI

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento.

In caso di anomalie, l'azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree (di norma Direzioni) nelle quali si è verificata l'anomalia.

In tali casi, il controllo si concluderà con un avviso al Responsabile della struttura dell'Area aziendale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

8 RESPONSABILITÀ E SANZIONI

L'utente, al fine di non esporre sé stesso e la Banca a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.

Gli utenti sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio, alla reputazione e alla clientela.

L'utente è responsabile per l'omessa erogazione della prestazione lavorativa causata dalla navigazione Internet ingiustificata e/o non autorizzata ovvero protratta oltre il tempo strettamente indispensabile all'espletamento delle operazioni connesse allo svolgimento dell'attività lavorativa.

Tutti gli utenti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;
- per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.