Regolamento per i servizi infotelematici

S.C.R. PIEMONTE S.p.A.
Società di Committenza Regione Piemonte
società per azioni con socio unico
sede corso Marconi 10 – 10125 Torino
cap.soc. € 1.120.000,00 i.v.
rea della CCIAA di Torino n. 1077627
c.f. e p. iva 09740180014 – www.scr.piemonte.it

PRESIDENZA
tel. +39 011 6548300
fax +39 011 6694665
presidenza@scr.piemonte.it

1 Premessa

La sicurezza delle informazioni ha il compito di tutelare la **riservatezza** (assicurare che le informazioni siano accessibili solo a che è autorizzato), l'**integrità** (assicurare che i dati possano essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione) e la **disponibilità** (assicurare che l'informazione ed i servizi informatici devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio) delle informazioni, riducendo ad un livello accettabile il rischio di perdita, modifica o indisponibilità.

Deve essere inoltre garantita la **conformità** dei sistemi informativi rispetto ai requisiti di sicurezza previsti dall'ordinamento giuridico, ed in particolare D.Lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" (di seguito **"Codice Privacy"**). Ogni attività prevista nel presente Regolamento deve essere posta in essere nel rispetto della predetta normativa e relativi regolamenti attuativi.

Le attività per il raggiungimento di tale obiettivo sono complesse ed articolate e richiedono una continua evoluzione. Una corretta attuazione è possibile solo attraverso la collaborazione di tutti i soggetti coinvolti. E' inoltre fondamentale il coordinamento ed il monitoraggio delle attività di sicurezza correnti e di innovazione tecnologica, soprattutto qualora affidate a fornitori esterni, anche attraverso una corretta identificazione dei ruoli e delle responsabilità dei fornitori dei servizi e degli utenti del sistema sulla consapevolezza e sensibilizzazione del personale attraverso il continuo aggiornamento delle politiche di comportamento da tenere nell'utilizzo degli strumenti informatici.

2 Ruoli e Responsabilità Generali

2.1 Presidente del Consiglio di Gestione e Referente Informatico

Il Presidente del Consiglio di Gestione di SCR Piemonte S.p.A., avvalendosi del supporto del Referente Informatico:

a) determina le necessità di accesso ai Sistemi Informativi da parte degli utenti, effettuando le procedure stabilite per l'attivazione secondo il profilo di autorizzazione opportuno e per la disattivazione nel momento in cui viene a cessare la necessità;
b) controlla l'applicazione delle politiche di sicurezza delle informazioni, assicurando che ciascun dipendente si attenga a comportamenti idonei per l'utilizzo degli strumenti informatici;
c) diffonde a tutto il personale le politiche di sicurezza delle informazioni;
d) controlla l'applicazione delle politiche di sicurezza delle informazioni, assicurando che ciascun dipendente contribuisca alla sicurezza delle informazioni attenendosi a comportamenti idonei e corrispondenti a quanto definito nelle politiche per l'utilizzo degli strumenti informatici;
e) sensibilizza gli utenti alla comunicazione tempestiva, alle strutture preposte, di ogni incidente o rischio in materia di sicurezza informatica, in modo tale che possano essere presi gli opportuni provvedimenti.

2.2 Gestori Esterni

Il **ruolo** dei Gestori Esterni di servizi di Information and Communication Technology (nel prosieguo ICT) per la gestione della sicurezza delle informazioni consiste nel:

a) predisporre le misure tecniche, gestionali e procedurali atte a ridurre i rischi di sicurezza attraverso azioni preventive di gestione delle vulnerabilità e attraverso azioni di mitigazione dell'impatto;
b) controllare che, in caso di variazioni alla configurazione dei sistemi, sia verificata l'adeguatezza delle funzionalità, anche dal punto di vista della sicurezza delle informazioni;
c) segnalare a SCR Piemonte eventuali situazioni anomale o incidenti sui servizi erogati, applicare le opportune attività correttive e fornirne un adeguato resoconto in funzione della severità dell'accadimento;
d) identificare i problemi relativi alla sicurezza informatica e risalire alle cause primarie, anche attraverso l'analisi di trend o dell'insieme di incidenti rilevanti, e proporre al Referente Informatico azioni correttive ai problemi identificati;
e) fornire, su richiesta, resoconti sullo stato della sicurezza informatica al Referente Informatico.

In particolare il **Gestore Servizi di Rete:**

f) stabilisce in accordo con il Referente Informatico, ed implementa, le misure di sicurezza della rete e ne verifica le funzionalità;
g) monitora costantemente il traffico di rete individuando potenziali vulnerabilità ed incidenti;
h) individua le cause primarie di disservizi che hanno compromesso la funzionalità del sistema e lo comunica al Referente Informatico;

2.3 Gestore interno delle Postazioni di lavoro (di seguito PdL)

i) **Il** Referente Informatico:configura ed aggiorna le PdL e i Server in modo tale da minimizzare i rischi per la sicurezza delle informazioni;
j) verifica la presenza di virus, procede a rimuoverli per garantire la sicurezza della rete e rendere operativa la PdL ristabilendo le condizioni generali di sicurezza;
k) gestisce le utenze per l'accesso alla PdL ed alle risorse di rete del dominio di SCR Piemonte;
l) gestisce la cancellazione sicura delle PdL da dismettere o da riassegnare ad un altro utente in linea con la normativa dettata dal Garante per la Privacy.

2.4 Utenti

Il ruolo degli **utenti** di SCR Piemonte, siano essi dipendenti o collaboratori, consiste nel:

a) operare in maniera responsabile, secondo le regole descritte nel paragrafo "Modalità di utilizzo degli strumenti informatici" per la tutela della riservatezza, della protezione dei dati, dell'etica comportamentale e dell'utilizzo corretto degli strumenti informatici messi a disposizione da SCR Piemonte;
b) segnalare tempestivamente qualunque evento si ritenga un potenziale incidente alla sicurezza informatica (aggressioni da virus informatici, attacchi da malintenzionati interni o esterni, siti web fasulli, ecc.), al Referente Informatico;
c) segnalare tempestivamente lo smarrimento o la sottrazione dell'attrezzatura personale in dotazione.

3 Principi e Politiche

I principi basilari ai quali SCR Piemonte si attiene per quanto riguarda l'attuazione delle misure atte a garantire la sicurezza delle informazioni, sono costituiti da:

a) **Presidio globale della sicurezza:** deve essere assicurata una visione unitaria e strategica a livello di Amministrazione in grado di valutare sia il rischio operativo complessivo sia le necessarie misure di sicurezza;
b) **Corretta responsabilizzazione:** la valutazione del rischio e la realizzazione della sicurezza necessaria devono essere garantite dai ruoli dell'Amministrazione dotati di responsabilità e di autonomia, anche a livello di delega, nonché di conoscenza dell'operatività per prendere decisioni chiave;
c) **Bilanciamento rischio/sicurezza:** qualsiasi investimento per la realizzazione di contromisure di sicurezza deve essere quindi rigorosamente collegabile al margine del rischio ottenibile mettendo in campo quelle contromisure;
d) **Separazione dei compiti:** vale il principio secondo il quale chi verifica non deve essere chi ha eseguito il compito o l'obiettivo assegnato.

Per raggiungere gli obiettivi sopra indicati, il presente documento comprende le regole atte a definire il corretto comportamento nell'uso della strumentazione informatica.

3.1 Modalità di utilizzo degli strumenti informatici

I beni che compongono il sistema informativo rappresentano una componente vitale per l'operatività di SCR Piemonte e, pertanto, un utilizzo consapevole degli strumenti informatici rappresenta una condizione imprescindibile e un obiettivo prioritario da perseguire. A tal fine, vengono individuate l'insieme di regole atte a definire il corretto comportamento da tenere nell'utilizzo dei dispositivi messi a disposizione da SCR Piemonte.

3.1.1 Norme Generali di comportamento

Tutti gli utenti ai quali è stata assegnata una postazione di lavoro (PdL) fissa o mobile, telefoni fissi o cellulari o altro bene informatico, devono attenersi alle regole di comportamento di seguito elencate:

a) gli strumenti assegnati, compresi i relativi programmi, i servizi di posta elettronica e l'accesso alla rete Internet, nonché le unità di rete messe a disposizione per la condivisione delle informazioni, sono strumenti di lavoro di proprietà di SCR e, pertanto devono essere utilizzati per motivi attinenti alla prestazione lavorativa. E' consentito uno sporadico ed occasionale utilizzo anche a scopi personali, purchè questo sia circoscritto nei tempi di pausa previsti dal D.Lgs. n. 66/203 ("Attuazione delle direttive 93/104/CE e 2000/34/CE concernenti taluni aspetti dell'organizzazione dell'orario di lavoro"); tale sporadico ed occasionale utilizzo – che non deve gravare eccessivamente sulle risorse di SCR (es. sovraccarico alla rete) e non deve altresì compromettere il funzionamento o la sicurezza dei sistemi informativi di SCR medesima – deve avvenire nel rispetto delle regole di comportamento indicate nei paragrafi "uso consapevole di Internet" e "uso consapevole della posta elettronica" indicate successivamente;

b) lo scambio di messaggi di posta elettronica per scopi non lavorativi deve essere effettuato da una casella personale differente da quella fornita da SCR; a tale scopo possono essere utilizzati servizi di posta disponibili ed accessibili via Web;
c) l'utente deve trattare le informazioni in modo lecito e secondo correttezza raccogliendole e registrando solo per scopi inerenti all'attività svolta ovvero per le finalità previste dalle mansioni assegnate e secondo i profili e le autorizzazioni concesse;
d) l'utente deve trattare in modo lecito il materiale protetto da proprietà intellettuale in qualunque sua forma (testi, immagini, programmi, ecc.), non deve quindi fare uso di tale materiale (visione, copia, conversione, reinoltro ecc.), anche solo di parte di esso se non nei termini concessi dalle vigenti normative o dalle condizioni di utilizzo. L'utente deve altresì operare garantendo la riservatezza necessaria alle informazioni di cui viene a conoscenza, custodendole con diligenza e non divulgandole a persone non autorizzate;
e) in caso di allontanamento dalla postazione di lavoro (PdL) è necessario bloccare l'accesso al proprio personal computer per impedirne l'utilizzo ad altri utenti;
f) per i dispositivi mobili (es. telefoni cellulari, ecc.), dato il forte utilizzo in mobilità ed il maggiore rischio di smarrimento e furto, l'utente deve prevedere l'abilitazione di un codice di protezione del dispositivo in tutti i casi ove sia possibile;
g) in caso di accertato utilizzo improprio della strumentazione o di utilizzo per fini diversi da quelli consentiti per esigenze di lavoro, l'Amministrazione provvederà ad applicare, nei confronti dell'utente, le norme disciplinari previste dal CCNL vigente;
h) l'installazione o l'uso di programmi o componenti hardware diversi da quelli forniti è consentita solo se preventivamente autorizzata dal Referente Informatico e previa verifica di compatibilità;
i) si richiede particolare attenzione nell'utilizzo e nella custodia dei dispositivi mobili, quali ad esempio pc portatili, telefoni cellulari, ecc., affinchè non vi sia perdita o furto di informazioni critiche o il dispositivo stesso non venga rubato. E' a cura dell'utente effettuare regolarmente operazioni di archiviazione (backup) delle informazioni importanti, nonché garantire la protezione delle informazioni riservate;
j) deve essere prontamente data comunicazione, tramite mail, al Referente Informatico, di eventuali furti, danneggiamenti o smarrimenti della strumentazione assegnata o parte di essa; inoltre l'assegnatario dovrà recarsi (personalmente e al più presto) presso un Commissariato di PS o Stazione CC per sporgere regolare denuncia: copia della stessa dovrà essere fatta pervenire al Referente Informatico;
k) quando uno strumento informatico non è più utilizzato da un assegnatario, lo stesso deve segnalarlo tempestivamente al Referente Informatico, che provvederà a rendere disponibile la risorsa o la sua dismissione.

3.1.2 Gestione delle credenziali per accesso a PdL, dispositivi mobili e altre applicazioni

La credenziali di autenticazione consistono in un codice per l'identificazione dell'utente associato a una parola chiave riservata e conosciuta solo dal medesimo. Una corretta gestione delle credenziali prevede che:

a) le credenziali siano in possesso e uso esclusivo dell'utente;

b) ad ogni utente sono assegnate o associate individualmente una o più credenziali per l'autenticazione;
c) con le istruzioni impartite agli utenti è prescritto di adottare le necessarie cautele per assicurare la segretezza della credenziale e la diligente custodia dei dispositivi in possesso ad uso esclusivo dell'incaricato;
d) la parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; non contiene riferimenti agevolmente riconducibili all'utente ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi;
e) Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri utenti, neppure in tempi diversi;
f) Le credenziali di autenticazione dell'utente non più utilizzate sono disattivate, salvo quelle preventivamente autorizzate per i soli scopi di gestione tecnica;
g) Le credenziali sono disattivate in caso di perdita della qualità che consente all'utente l'accesso ai dati personali;
h) Sono impartite istruzioni agli utenti per non lasciare incustodito e accessibile lo strumento elettronico;
i) in caso di prolungata assenza o impedimento dell'utente che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività, l'utilizzo delle credenziali è organizzato garantendo la relativa segretezza e individuando preventivamente i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'utente dell'intervento effettuato;

3.1.3 Uso consapevole di Internet

L'utilizzo di Internet avviene mediante la rete regionale RUPAR Piemonte che permette l'accesso al Web. L'utilizzo di Internet è consentito per lo svolgimento delle operazioni legate all'attività lavorativa. La rete regionale, pur essendo protetta, è comunque soggetta a rischi, i principali dei quali sono legati a:

a) utilizzo improprio delle risorse;
b) accesso a siti non idonei;
c) possibili attacchi provenienti da codice maligno (virus, worm, cavalli di Troia, ecc.);
d) mancato rispetto della legislazione sul diritto d'autore.

Oltre alle misure tecniche (es. antivirus, sistema di filtri che impedisce l'accesso a siti considerati pericolosi o non correlati con la prestazione lavorativa) è necessario che l'utente adotti comportamenti ai fini della protezione delle risorse assegnate e delle informazioni e segnatamente:

e) il nome utente e la password utilizzati per l'accesso Windows al PC che consente l'accesso a Internet devono essere tenuti riservati e non possono essere condivisi con altri utenti;
f) e' vietato scaricare ed installare programmi non espressamente autorizzati anche se in forma gratuita, poiché potrebbero contenere un codice malevolo;
g) nell'uso dei social network (es. Facebook, Twitter, Linkedin), attivo dalle ore 12 alle ore 14, data la caratterizzazione di tali servizi, è sconsigliato pubblicare informazioni inerenti l'attività lavorativa, in quanto potrebbero essere viste da persone non autorizzate.

3.1.4 Uso consapevole della Posta Elettronica

La posta elettronica è diventata uno strumento fondamentale nello svolgimento dell'attività lavorativa e, pertanto, occorre osservare alcune precauzioni per evitare che le e-mail scambiate causino rischi ai servizi informativi o contribuiscano a diffondere informazioni riservate. Si ricorda inoltre che il materiale ed i contenuti inviati sono sotto diretta responsabilità dell'utente e che non è permesso inviare messaggi che ledano l'immagine di SCR.

Vengono di seguito descritte le principali regole di comportamento:

a) la casella di posta tramite interfaccia Web, con i relativi messaggi è gestita sui server del gestore esterno del servizio; la casella di posta elettronica certificata (MS Outlook), di dimensione limitata, è replicata anche sul server di SCR Piemonte ed è gestita dall'ICT di SCR;
b) l'ambiente di posta limita la dimensione massima di un messaggio e degli allegati sia in invio che in ricezione. Per tale motivo prima di allegare un documento di grosse dimensioni si consiglia di effettuare la compressione. Inoltre nel caso di più documenti da allegare, se ne consiglia la compressione in un unico file;
c) l'ambiente di posta riesce ad identificare ed eliminare i principali virus nascosti negli allegati; tuttavia è sempre possibile che qualche virus non venga intercettato. E' consigliato quindi cancellare ogni e-mail con allegati sospetti specialmente se non se ne conosce la provenienza;
d) è vietato rispondere alla posta indesiderata (spam) o a messaggi che chiedono di effettuare operazioni che comportano l'inserimento dei dati utente e password in quanto potrebbero contribuire alla diffusione e generazione di altra posta indesiderata;
e) è vietato l'invio di allegati con dimensioni eccessive o ad un numero elevato di destinatari se non strettamente necessario. La spedizione di allegati di dimensioni eccessive o l'invio di e-mail ad un numero elevato di destinatari possono compromettere il funzionamento del servizio;
f) è buona norma, in caso di assenze prolungate per ferie o altro, attivare un messaggio automatico che indica il periodo di assenza ed eventualmente un altro riferimento al quale inviare i messaggi di lavoro urgenti.

3.1.5 Salvataggio e condivisione dati

Le informazioni ed i documenti elaborati dagli utenti devono essere a disposizione dell'Amministrazione.

Il salvataggio di tutti i dati gestiti sul server, sia quelli trattati singolarmente da ciascun utente, sia quelli trattati in condivisione tra più utenti in funzione della struttura organizzativa di SCR, viene effettuato, in automatico, ogni giorno, in orario notturno.

È a carico degli utenti effettuare il backup di eventuali dati aziendali gestiti sul proprio pc.

3.1.6 Gestione dei supporti rimovibili

Gli utenti devono prestare la massima attenzione nell'uso dei supporti rimovibili di memorizzazione.

In caso di utilizzo di supporti rimovibili valgono le seguenti linee guida:

a) chi registra le informazioni su questo tipo di supporti è responsabile della custodia e deve operare in modo da evitare la lettura dei dati da parte di persone non autorizzate;
b) non appena viene meno la necessità di mantenere i dati su supporto rimovibile occorre provvedere alla loro cancellazione irreversibile.
c) tutti i supporti di memorizzazione destinati a contenere dati riservati, se lasciati in ufficio, devono essere collocati in armadi chiusi con adeguati sistemi di protezione (accesso mediante chiave).

3.1.7 Amministratore di sistema

Non sono concessi diritti di amministratore sulle PdL. La concessione di tali diritti avviene solo in casi eccezionali e deve essere esplicitamente richiesta, con le opportune motivazioni ed autorizzata, se effettivamente necessaria, dal Referente Informatico.

All'utente a cui è concesso il diritto di amministratore è pertanto richiesto di:

a) informare preventivamente il Referente Informatico relativamente a tutti i software che intende installare;
b) garantire che non siano modificati né disabilitati i software standard (antivirus, office, file di sistema, ecc);
c) rispettare le regole di sicurezza adottate da SCR Piemonte (divieto di modificare le impostazioni di accesso alla rete o l'indirizzo IP; divieto di modificare le politiche di sicurezza del PC; divieto di condivisione di cartelle ospitate esclusivamente sul PC).

3.1.8 Assenza improvvisa o prolungata

In caso di assenza improvvisa o prolungata di un utente e per improrogabili necessità operative si renda necessario accedere alla sua Pdl, per recuperare informazioni o documenti, si applica la seguente procedura:

a) il responsabile della risorsa interessata invia in forma scritta o tramite e-mail al Presidente del Consiglio di Gestione una richiesta di autorizzazione ad accedere ai dati dell'utente con la relativa motivazione ed il dettaglio delle informazioni necessarie;
b) il responsabile, a fronte dell'ottenimento delle autorizzazioni necessarie, provvede a:
   - inoltrare la richiesta al Referente Informatico che provvederà ad individuare un amministratore di sistema che effettui l'intervento;
   - informare tempestivamente l'utente dell'intervento necessario tramite telefono in prima istanza, quindi per telegramma;
c) l'amministratore di sistema per l'intervento:
   - effettua il recupero delle informazioni necessarie eventualmente supportato dal responsabile richiedente;
   - redige un verbale dell'intervento effettuato che sarà inviato a mezzo e-mail al responsabile che ha richiesto l'intervento;
   - procede alla modifica delle password in modo tale da non consentire successivi accessi;
d) il responsabile trasmette il verbale dell'intervento al Presidente del Consiglio di Gestione ed all'utente, alla prima occasione utile.

4 Assegnazione delle attrezzature e dei servizi informatici

Le attrezzature HW e SW sono assegnate dietro esplicita richiesta scritta da inoltrare al Referente Informatico da parte del responsabile della risorsa assegnataria delle attrezzature.

Nel momento in cui una persona assegnataria di un qualunque bene informatico non dovesse più necessitarne, lo dovrà segnalare, attraverso il proprio responsabile, al Referente Informatico, che provvederà a effettuare l'opportuno ritiro.

4.1.1 Personal Computer

Il Personal Computer (PC) è uno strumento di lavoro considerato indispensabile.

Ai dipendenti, ai collaboratori (co.co.co. e co.co.pro.), agli stagisti, ai borsisti viene attribuita una PdL fino alla scadenza del contratto sottoscritto con SCR; alla scadenza del contratto, la PdL verrà riassegnata ad altre figure professionali.

Non è prevista l'assegnazione di un PC o di altri servizi informatici ad altre figure professionali ad eccezione di manifesta necessità e comunque su approvazione da parte del Referente Informatico.

4.1.1.1 Criteri di assegnazione

Ad ogni profilo professionale sopra indicato è assegnata un'unica postazione che può essere o un PC desktop (postazione fissa) oppure un PC Portatile accessoriato.

4.1.2 Stampanti

Si individuano le seguenti tipologie di stampanti:

- stampanti di rete;
- stampanti locali.

I criteri per la distribuzione delle stampanti tengono in considerazione prioritariamente la collocazione del personale, quindi rispettano criteri logistici.

In particolare:

a) nelle aree comuni di stampa sono installate le stampanti di rete B/N e a colori;

b) a ciascun Dirigente è assegnata una stampante locale.

4.1.3 Fax

Per l'invio di Fax sono disponibili le apparecchiature dislocate presso le singole Direzioni e/o Funzioni aziendali.

4.1.4 Posta elettronica

Tutte le caselle di Posta Elettronica sono configurate per l'utilizzo tramite interfaccia Web, ad eccezione delle caselle di posta certificata che sono configurate per l'utilizzo in ambiente Microsoft Outlook.

Al personale in servizio è attribuita d'ufficio una casella di posta elettronica nominativa. Non è ammessa più di una casella di posta elettronica nominativa per dipendente, collaboratore, stagista o borsista.

Le caselle di posta elettronica nominative, compreso il contenuto, hanno validità temporale coincidente con la permanenza in servizio della persona fisica alla quale sono attribuite e vengono archiviate per una durata massima di dieci anni dopo la conclusione del rapporto di lavoro.

Le caselle di gruppo sono attivate ed aggiornate in occasione dell'adozione e/o della modifica dell'organigramma aziendale, previa richiesta scritta del Referente Informatico da inoltrarsi a mezzo e-mail ai Responsabili delle funzioni aziendali interessate, dell'indicazione di un responsabile di dette caselle, dei nomi delle persone che possono accedervi e delle regole di autorizzazione (solo lettura, lettura/scrittura; lettura/scrittura/cancellazione/archiviazione ecc..).

Le caselle di gruppo non più utilizzate vengono cancellate previo trasferimento delle stesse e del relativo contenuto in apposito sistema di archiviazione per una durata massima di dieci anni.

E' inoltre possibile, in casi limitati ed in presenza di adeguate motivazioni, richiedere al Referente Informatico l'attivazione di specifiche caselle di posta (non nominative e di gruppo) con l'indicazione di un responsabile di dette caselle, dei nomi delle persone che possono accedervi e delle regole di autorizzazione. Dette caselle di posta possono essere cancellate d'ufficio se non vengono utilizzate per oltre 1 anno, previa comunicazione al responsabile della casella medesima; prima della cancellazione le caselle ed il loro contenuto sono trasferite in apposito sistema di archiviazione per una durata massima di dieci anni.

4.1.5 Accesso Internet

Per il personale in servizio presso SCR è fornito l'accesso alla rete Internet tramite user name e password utilizzate per l'accesso Windows al PC.

4.1.6 Software

Con la PdL sono installati e configurati software di base comuni a tutti gli utenti. L'assegnazione di ulteriori software e/o dell'eventuale accesso ad applicativi sono legati alle funzioni assegnate ed agli incarichi ricoperti e deve essere effettuato tramite richiesta al Referente Informatico. E' fatto divieto di

installare software senza la previa autorizzazione del Referente Informatico. Tutto il software installato sulle PdL deve essere preventivamente testato per verificarne la compatibilità.

Nel caso si necessiti l'installazione di un software non testato, esso dovrà essere sottoposto preventivamente a verifica. Per effettuare tale operazione potrebbe essere necessaria la collaborazione del richiedente e/o del fornitore del software.

La richiesta di installazione del software non standard, sia provvisto di una regolare licenza d'uso, sia ad utilizzo gratuito, viene valutata dal Referente Informatico. Nel caso venga identificato un software standard con caratteristiche analoghe già utilizzato in SCR, questo verrà proposto all'utente.

4.1.7 Spazio Memoria di Rete

Per il salvataggio dei dati sia personali che condivisi, residenti sui server, sono disponibili dei supporti per il backup, che viene effettuato ogni giorno, in orario notturno, per cui in casi di perdita dei dati si potrà richiederne il ripristino.

5 Assegnazione delle attrezzature e dei servizi di fonia fissa e fonia dati mobile

Gli apparecchi telefonici fissi, i telefoni cellulari e i servizi ad essi collegati, che sono in dotazione a SCR sono gestiti tramite accordi contrattuali con gestori esterni.

5.1 Criteri relativi all'assegnazione dei servizi di telefonia fissa

A tutto il personale di SCR viene assegnato un numero ed un apparecchio telefonico. Tutti i numeri telefonici attivati sono abilitati alle chiamate aziendali, nazionali e cellulari. Gli apparecchi forniti sono quelli selezionati dal Referente Informatico.

5.1.1 Mobilità del personale

In caso di mobilità del personale per cambio di competenze, l'utente conserva il proprio numero telefonico. Fanno eccezione i numeri legati a servizi particolari in cui è importante che il numero di telefono resti invariato (ad esempio le segreterie, ecc.), in questi casi all'utente sarà assegnato un nuovo numero di telefono.

5.2 Criteri relativi all'assegnazione dei servizi di telefonia mobile

Il gestore dei servizi di telefonia mobile mette a disposizione di SCR un listino di apparecchi e servizi disponibili.

5.2.1 Assegnazione utenze telefoniche

Sono assegnate utenze telefoniche e relativi apparecchi cellulari ai Dirigenti ed ai Quadri aziendali.

Incluso nel servizio di fonia mobile, è prevista una quantità limitata di traffico dati mensile per navigare in Internet. E' in carico all'utente assegnatario la gestione responsabile del servizio affinchè il consumo del traffico sia correttamente distribuito all'interno del mese.

5.2.2 Accettazione e responsabilità delle utenze e degli apparecchi telefonici

Per ogni utenza mobile, l'assegnatario deve firmare il modulo predisposto dal Referente Informatico.

Dal momento della firma, il diretto titolare dell'utenza ne risponde a tutti gli effetti (indagini, costi, utilizzi, furti e smarrimenti, mancata consegna dopo la cessazione del rapporto di lavoro, ecc.).

In caso di furto/smarrimento dell'apparecchio telefonico e/o della sim aziendale, l'assegnatario dovrà seguire quanto indicato all'interno del capitolo "Norme Generali di Comportamento".

5.2.3 Telefonate personali effettuate con utenza cellulare aziendale

Tutti gli utenti che hanno in dotazione un'utenza telefonica cellulare aziendale, possono utilizzarla per le chiamate personali, avendo cura di utilizzarla in modo consapevole e responsabile senza eccedere nell'utilizzo.

6 Verifica dati di traffico telefonico fisso e mobile

La verifica del traffico telefonico fisso e mobile viene effettuata dal Referente Informatico al ricevimento della fattura emessa dal gestore del servizio.

7 Misure di protezione principali

7.1.1 Postazioni di lavoro (PdL)

Sistema Antivirus

Tutte le PdL che hanno accesso alla rete (dominio scr.locale) sono dotate si sistema antivirus per il rilevamento, segnalazione, blocco e rimozione di virus, worm, Trojan, adware e altre applicazioni pericolose o indesiderate.

La distribuzione degli aggiornamenti è completamente automatizzata.

Una consolle centralizzata permette di monitorare tutte le attività di aggiornamento in atto, verificarne il completamento e le relative segnalazioni del virus al fine di intervenire in modo opportuno e mirato per evitare pericoli di ulteriore diffusione del virus.

Configurazioni di sicurezza

Le policy di protezione dei dati e dei profili utente per l'accesso alle risorse condivise del dominio sono contenute in Active Directory.

Profili utente e autorizzazioni

L'accesso alla PdL ed al dominio da parte degli utenti del sistema informativo di SCR è effettuato con privilegi di tipo "utente" che non permette l'installazione di prodotti software e la modifica dei privilegi assegnati.

Aggiornamenti e patch di sicurezza

Le PdL prevedono un sistema centralizzato ed automatizzato per la distribuzione degli aggiornamenti relativi al Sistema Operativo.

Interventi di assistenza

Gli interventi di assistenza sulla PdL dell'utente possono richiedere l'accesso da remoto: Tale mdolalità di accesso può avvenire unicamente con il consenso dell'assegnatario dell PdL, che viene richiesto contattando direttamente l'utente.

Dismissione delle PdL

Su tutti i PC che esauriscono il proprio ciclo di vita si procede alla cancellazione sicura dei dati affinchè non possano essere recuperati; successivamente vengono rottamati mediante affidamento ad una ditta esterna specializzata.

7.1.2 Posta elettronica

Il servizio di posta elettronica prevede specifiche misure di protezione, che attraverso l'analisi automatica del contenuto della mail identificano virus, worm o altre minacce. E' presente inoltre un sistema automatico che contrassegna le mail di posta indesiderata (spam).

Il Gestore esterno del servizio di posta elettronica effettua regolarmente l'archiviazione del contenuto delle caselle di posta, fino ad un massimo di 10 anni. Qualora l'utente ne avesse necessità è possibile richiedere il ripristino dal backup. Solo l'utente interessato può avere accesso alle proprie informazioni contenute nel backup.

La riservatezza dell'accesso alla posta elettronica è garantito mediante un codice di identificazione utente (login) e password rilasciate dal gestore esterno in fase di configurazione della casella di posta e sono da utilizzarsi per l'accesso Web alla posta elettronica. Al primo accesso è richiesto di effettuare il cambio della password, che successivamente dovrà essere modificata in base alle policy aziendali vigenti.

Il gestore del servizio di posta elettronica, inoltre, dispone di strumenti di monitoraggio del traffico che possono mettere in evidenza anomalie che possano comprometterne il funzionamento.

Un sistema di gestione della posta indesiderata (sistema anti-spam) filtra tutte le mail che vengono inviate dall'esterno e blocca gran parte della posta indesiderata o insicura.

7.1.3 Internet

L'accesso ad Internet è regolamentato da un insieme di misure a tutela della sicurezza. Le strategie di protezione prevedono:

a) l'utilizzo di uno sbarramento per impedire l'accesso dall'esterno ed un filtro di accesso dalla rete interna a quella esterna;
b) l'uso di un sistema di autenticazione centralizzato;
c) l'utilizzo di un server proxy per il controllo degli accessi alla rete Internet e per il filtraggio dei contenuti provenienti dal Web.

Tuttavia, nonostante le forme di prevenzione attuate, non è escluso che l'utente, durante la navigazione, possa imbattersi in potenziali minacce informatiche, in materiale non appropriato e/o Indesiderato.

7.1.4 Risorse di Rete e Accesso al Dominio

Per proteggere le informazioni che transitano nella rete e nella stessa infrastruttura di supporto vengono individuati specifici controlli e metodologie per assicurare un utilizzo sicuro dei servizi di rete. La rete è gestita e controllata adeguatamente per garantire la sicurezza dei sistemi e delle applicazioni che la utilizzano, per proteggere la rete da accessi non autorizzati.

La sicurezza della rete è regolamentata dall'attuazione di specifiche misure quali:

a) protezione dei locali dove sono custoditi gli apparati di rete;
b) aggiornamento all'ultima versione degli apparati attivi;
c) ridondanza delle connessioni fisiche e degli apparati critici;
d) salvataggio periodico dei dati di configurazione degli apparati di rete;
e) Configurazione dei server secondo politiche che garantiscano i requisiti di legge.

7.1.5 Verifiche sicurezza e procedure in caso di incidente

SCR può utilizzare gli strumenti utili a verificare situazioni specifiche di anomalie che comportano un rischio alla sicurezza delle informazioni (es. vulnerabilità del sistema operativo e configurazioni non consone, presenza log di sicurezza) e non conformità con le politiche tecniche definite (es. software non standard), Tali verifiche possono avvenire unicamente nel rispetto dei principi di pertinenza, non eccedenza rispetto alle finalità e gradualità, secondo quanto stabilito dalla normativa vigente sulla Privacy.

In caso di incidente di sicurezza (es. infezione da virus) il personale tecnico incaricato può procedere con le seguenti azioni:

a) Bloccare l'accesso degli strumenti assegnati alla rete di SCR o alcuni servizi mirati per arginare l'incidente;
b) Effettuare analisi specifiche sulla PdL o altro bene assegnato per identificare la natura del problema e pianificare le opportune contromisure.

In particolare, tali analisi devono avvenire, preferibilmente, in loco con la presenza dell'utente; qualora l'utente interessato non sia presente e l'intervento sia inderogabile, deve essere autorizzato dal Referente Informatico.

Verrà redatto un verbale di quanto effettuato e reso noto all'utente alla prima occasione utile.

L'utente interessato e SCR dovranno collaborare affinchè i tecnici possano svolgere rapidamente ed efficacemente le operazioni derivanti dall'incidente ed effettuare al più presto il ripristino alla situazione normale.

Il Referente Informatico, in collaborazione con i fornitori ICT, si riserva la possibilità di attivare analisi a campione, limitate nel tempo, sugli accessi ai Sistemi per verificare e prevenire eventuali incidenti di sicurezza.