C O M U N E D I A S S O R O

Provincia Regionale di Enna

REGOLAMENTO PER L'UTILIZZO DELLE TECNOLOGIE DELL'INFORMAZIONE E DELLE COMUNICAZIONI (ICT) IN RETE, EFFETTUATO TRAMITE POSTA ELETTRONICA ED INTERNET

Approvato con delibera di C.C. n. 42 del 22.09.2014

Art. 1
Principi generali

Le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti. Definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.

Art. 2
Responsabile delle comunicazioni

1. Il Titolare del trattamento, di seguito Titolare, individua il Responsabile delle comunicazioni in rete, di seguito Responsabile, quale figura deputata alla organizzazione, gestione e verifica delle disposizioni contenute in questo regolamento. Il Responsabile verrà nominato con atto separato nel quale verrà fatto riferimento a questo regolamento relativamente alle mansioni attribuitegli.

2. Gli incaricati del trattamento, di seguito incaricati, dovranno attenersi strettamente alle disposizioni emanate dal Responsabile.

Art. 3
Individuazione delle risorse

1. Il Responsabile provvede alla formazione dell'inventario delle risorse, ricomprendendo i componenti hardware, software e le banche dati.

2. Il Registro delle risorse deve prevedere almeno i seguenti campi:

- l'area/servizio a cui è assegnata la risorsa
- il responsabile che ha autorizzato l'ingresso/uscita
- data dell'autorizzazione concessa

Art. 4
Autenticazione

1. Gli incaricati che accedono ai sistemi di comunicazione dovranno essere dotati di un sistema di autorizzazione costituito da nome utente e password.

2. Il Responsabile attiverà l'incaricato della manutenzione per la predisposizione delle autenticazioni. Si farà carico inoltre di redigere un documento indirizzato agli utenti sulle disposizioni relative alle caratteristiche che dovranno avere le password che qui riassumiamo:

- devono essere costituite da almeno otto caratteri
- non devono contenere riferimenti riconducibili all'incaricato
- devono essere modificate dall'incaricato al primo utilizzo
- devono essere successivamente modificate almeno ogni tre mesi

3. Verificherà il rispetto dei requisiti sopraesposti tramite dei controlli a campione sulle password che vengono utilizzate con cadenza almeno semestrale e darà riscontro delle risultanze in un apposito registro.

4. In caso di risultanze difformi dalle disposizioni qui indicate, il Responsabile si curerà di rendere edotto l'incaricato di aver mancato ad un preciso obbligo di sicurezza e si assicurerà che lo stesso recepisca correttamente le indicazioni fornite.

5. Il Responsabile relazionerà annualmente al Titolare la percentuale di difformità riscontrate in modo da assicurare il mantenimento del livello di sicurezza richiesto nel corso del tempo.

6. Manterrà elenco dei codici identificativi che saranno assegnati curandosi di non farli più assegnare ad altri incaricati e verificherà semestralmente che le credenziali di autenticazione assegnate abbiano i requisiti per essere valide.

7. Attiverà l'incaricato della manutenzione per disattivare le credenziali di autenticazione non più valide, e si curerà di ricevere dichiarazione di conformità dell'intervento effettuato da allegare al registro dei codici identificativi.

Art. 5
Autorizzazione

1. Per l'accesso alle caselle di posta elettronica dell'ente devono essere individuati dei profili di autorizzazione che verranno assegnati agli incaricati.

2. I profili di autorizzazione potranno essere attribuiti sia a classi omogenee di incaricati che al singolo incaricato e verranno riportati in un apposito registro delle autorizzazioni a firma del Responsabile per la gestione delle comunicazioni.

3. Con cadenza annuale il Responsabile per la gestione delle comunicazioni in rete verificherà ed individuerà i profili di autorizzazione che siano eventualmente modificati, curandone la riassegnazione o la loro definitiva cancellazione ovvero la creazione di nuovi profili che siano necessari, ed il loro aggiornamento nel registro delle autorizzazioni.

4. Darà comunicazione formale all'incaricato della manutenzione dei sistemi informatici di attuare le modifiche necessarie e si curerà di ricevere dichiarazione di conformità dell'intervento effettuato da allegare al registro delle autorizzazioni.

Art. 6
Indisponibilità degli incaricati

1. Il Responsabile delle comunicazioni, in concerto con il soggetto incaricato alla manutenzione, dovrà individuare con relazione tecnica le risorse indispensabili per garantire l'operatività dei sistemi di comunicazione.

2. Dovrà inoltre indicare, in apposito documento, le casistiche e le tempistiche associate, che faranno attivare le procedure di emergenza.

3. Si curerà di rendere operativa la creazione di credenziali di autenticazione che abbiano possibilità di accedere alle risorse individuate nella relazione tecnica e individuerà per iscritto i soggetti incaricati della loro custodia.

4. Darà disposizioni agli incaricati ed alla società di manutenzione di avvisare tempestivamente l'ente in caso di loro impedimento e si coordinerà con l'ufficio Risorse Umane per gestire tali comunicazioni.

5. Darà, infine, comunicazione al Titolare in caso di suo impedimento che provvederà ad autorizzare un altro incaricato all'espletamento delle procedure di emergenza.

Art. 7
Rischi di intrusione o danneggiamento dei dati

1. Il Responsabile delle comunicazioni si attiva di concerto con l'incaricato dei servizi di manutenzione per individuare i dispositivi software ed hardware atti a proteggere i dati e i sistemi di comunicazione da programmi che possano danneggiarne, alterarne o interrompere il funzionamento.

2. L'individuazione di questi dispositivi dovrà essere motivata e formale, ed adeguata alle conoscenze tecniche possedute al momento dell'analisi. I dispositivi hardware e software individuati dovranno essere tenuti aggiornati con cadenza almeno semestrale di cui si dovrà tenere riscontro scritto.

3. Nel momento dell'aggiornamento dovrà essere verificata la validità delle scelte operate in precedenza e, se del caso, integrare o sostituire i dispositivi con altri che possano soddisfare meglio i requisiti di protezione richiesti.

4. Darà comunicazione formale all'incaricato della manutenzione dei sistemi informatici di attuare le modifiche necessarie e si curerà di ricevere dichiarazione di conformità dell'intervento effettuato.

Art. 8
Protezione dei sistemi da accessi abusivi

1. Il Responsabile delle comunicazioni si attiva di concerto con l'incaricato dei servizi di manutenzione per individuare i dispositivi che dovranno essere installati per la protezione dei sistemi informatici da accessi abusivi.
2. Dovranno essere verificati gli esiti delle configurazioni dei dispositivi di protezione e dovrà essere mantenuto riscontro scritto delle operazioni eseguite. Per le attività demandate all'incaricato della manutenzione dovrà essere richiesta dichiarazione di conformità degli interventi eseguiti.
3. Il Responsabile delle comunicazioni in rete si fa carico di inoltrare richiesta di riscontro al soggetto fornitore dei dispositivi di protezione delle attività di aggiornamento nella configurazione del software di protezione e del loro esito.

Art. 9
Aggiornamento dei programmi

1. Il Responsabile delle comunicazioni si attiva di concerto con l'incaricato dei servizi di manutenzione per individuare i programmi che dovranno essere soggetti ad aggiornamento periodico semestrale e le modalità di aggiornamento stesse.

2. Dovranno essere verificati gli esiti degli aggiornamenti e dovrà essere mantenuto riscontro scritto delle operazioni eseguite.

3. Per le attività demandate all'incaricato della manutenzione dovrà essere richiesta dichiarazione di conformità degli interventi eseguiti.

4. Il Responsabile delle comunicazioni si fa carico di inoltrare richiesta di riscontro al soggetto fornitore degli apparati hardware delle attività di aggiornamento del software di controllo e del loro esito.

Art. 10
Salvataggio dei dati

1. Il Responsabile delle comunicazioni in rete si attiva con i vari servizi per censire tutte le caselle di posta elettronica generiche che saranno sottoposte a salvataggio, includendo le caselle elettroniche PEC presenti.

2. Il Responsabile delle comunicazioni in rete provvederà ad individuare con provvedimento scritto i soggetti autorizzati alle procedure di backup avendo cura di trasmettere agli stessi le modalità tecniche di esecuzione e le tempistiche previste dal presente regolamento.

3. Il Responsabile delle comunicazioni in rete avvalendosi della consulenza dell'incaricato alla manutenzione esterna predisporrà le modalità di salvataggio dei dati a seguito di esame dei flussi di traffico rilevati, con tempistiche che non potranno superare i sette giorni. Le modalità di salvataggio e relative tempistiche dovranno essere sottoposte al Titolare del trattamento per la sua approvazione.

4. Il Responsabile delle comunicazioni in rete avvalendosi della consulenza dell'incaricato alla manutenzione esterna predisporrà le procedure di backup tenendo conto che una copia dei dati dovrà essere

conservata a disposizione per un accesso immediato nel sistema informativo di origine ed una copia dovrà essere riversata su supporto rimovibile.

5. Il Responsabile delle comunicazioni in rete individuerà un locale idoneo alla conservazione dei supporti rimovibili avendo cura di verificare che l'accesso sia ristretto ai soli soggetti autorizzati individuati con provvedimento scritto.

6. Il Responsabile delle comunicazioni in rete avvalendosi della consulenza dell'incaricato alla manutenzione esterna deve implementare una procedura di accesso alle copie conservate presso il sistema informativo di origine.

Art. 11
Formazione del personale

1. Il Responsabile delle risorse umane si attiva per individuare gli strumenti formativi più idonei relativamente all'organizzazione del lavoro presente nell'ente.

2. Il Responsabile delle risorse umane, di concerto con il Responsabile delle comunicazioni, stabilisce un programma formativo che preveda tempistiche, modalità di svolgimento e contenuti.

3. I contenuti del programma formativo dovranno prevedere almeno le seguenti tematiche:

- Rischi derivanti dall'utilizzo di uno strumento collegato ad internet
- Rischi derivanti dall'utilizzo della posta elettronica
- Rischi derivanti dall'utilizzo di un applicativo browser web
- Corretto utilizzo delle risorse dei punti precedenti
- Responsabilità derivanti da un utilizzo improprio degli strumenti con i quali si trattano i dati personali
- Procedure di sicurezza attualmente implementate nell'organizzazione
- Disciplina sulla protezione dei dati personali in rapporto alle relative attività

4. Copia del programma formativo, completo di tempistiche, modalità e contenuti dovrà essere inviata al Titolare del trattamento per sua approvazione preventiva.

5. Il programma formativo dovrà inoltre prevedere una verifica finale che attesti il livello di apprendimento finale acquisito e la predisposizione degli incaricati alle mansioni attribuite.

6. Il Responsabile delle risorse umane in concerto con il Responsabile delle comunicazioni si attiverà qualora il personale preposto vari a seguito di nuove assunzioni anche temporanee o a seguito di mobilità interna od esterna al fine di valutare l'eventuale ripetizione del ciclo formativo.

Art. 12
Politiche di sicurezza

1. Il presente articolo si applica a tutti i soggetti che hanno accesso diretto o indiretto ai dati. Si applica, inoltre, a tutti i soggetti esterni all'Ente, temporaneamente incaricati del trattamento dei dati.

2. Utilizzo di internet:

a) E' fatto divietodi scaricare ed installare software dalla rete internet senza la preventiva autorizzazione del Titolare.
b) E' fatto divieto di scaricare file musicali o video.
c) E' fatto divieto utilizzare software di P2P.

3. Utilizzo della posta elettronica:

a) L'utilizzo delle caselle di posta elettronica generiche è da ritenersi strumentale alla prestazione lavorativa, in caso di assenza del soggetto preposto, il contenuto delle stesse potrà essere visionato da un collega avente pari autorizzazioni lavorative interne per il corretto andamento dell'ufficio.
b) Posta elettronica personalizzata. L'utilizzo delle caselle di posta elettronica "nomedipendente.it" è da ritenersi strumentale alla prestazione lavorativa. Queste caselle avranno delle limitazioni in qualità e

quantità di allegati ed, in caso di assenza del dipendente, potrà essere permesso l'accesso ad un collega scelto dall'interessato stesso.

c) Viene fatto salvo e permesso l'utilizzodella posta elettronica personalizzata (nomeutente.it) per tutte le comunicazioni rientranti nelle relazioni sindacali e nel rapporto tra organizzazioni sindacali e lavoratori.
d) In nessun caso il servizio di posta elettronica è a beneficio del dipendente e potrà essere soggetto a modifiche o a sospensione in qualsiasi momento.

4. Verifiche e controlli dei sistemi:

a) Il titolare si riserva la facoltà di effettuare dei controlli anche saltuari od occasionali, per verifiche sulla funzionalità e sicurezza dei sistemi tramite registrazione di files di log sugli accessi ad internet ed al server di posta elettronica.
b) Come principio generale detti controlli verranno effettuati preliminarmente in forma aggregata e generale, nel caso venissero riscontrati abusi si procederà ad emettere un avviso di carattere generale relativo ad un rilevato utilizzo anomalo degli strumenti e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
c) In caso di abusi singoli, o reiterati, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni.

5. Conservazione dei dati personali:

a) Viene conservata copia dei dati personali anche sensibili relativi alle comunicazioni effettuate tramite posta elettronica limitatamente alla classe di indirizzi ufficio.it per un tempo comprendente il completo ciclo di trattamento dei dati personali coinvolti.
b) Viene conservata copia dei dati personali anche sensibili relativi alla navigazione internet effettuata tramite browser web o software similari, limitatamente ad un periodo temporale di 24 ore esteso a 48 ore in corrispondenza di periodi festivi o di vacanza lavorativa.
c) La conservazione delle copie dei dati personali anche sensibili potrà essere prolungata con atto motivato del Responsabile delle comunicazioni in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.
d) Su nomina del Responsabile delle comunicazioni vengono individuati gli incaricati al trattamento che saranno autorizzati ad accedere alle copie dei dati personali e sensibili.

Art. 13
Aggiornamento delle procedure

1. Il Responsabile, di concerto conla Società di manutenzione, si attiva entro il 31 marzo di ogni anno per la verifica e l'aggiornamento di tutte le procedure operative di cui ai precedenti articoli.

2. In particolare dovranno essere verificate e aggiornate le seguenti procedure:

- Procedure di autenticazione ed autorizzazione di cui all'artt. 4 e 5;
- Procedure per garantire la disponibilità dei sistemi di cui all'art. 6;
- Procedure per la protezione dei dati e dei sistemi di cui all'art. 7;
- Procedure per l'aggiornamento dei sistemi di cui all'art. 9;
- Procedure per il salvataggio dei dati di cui all'art.10.

3. Le eventuali proposte di variazione alle procedure dovranno essere motivate e formali e portate a conoscenza del Titolare del trattamento.

4. In caso di variazione alle procedure di cui al comma 2, il Titolare del trattamento conferisce incarico al Responsabile per l'attuazione. Il Responsabile dovrà integrare operativamente le nuove procedure e redigere una relazione tecnica sul buon esito delle operazioni.

INDICE: