Allegato B

REGOLAMENTO DELL'ASP AMBITO 9

Gestione e organizzazione dei Sistemi Informativi (IT)

Edizione 2023

Approvato con delibera del Consiglio di Amministrazione n. 46 del 29.08.2023

Sommario

REV. N.	§ REVISIONATI	DESCRIZIONE REVISIONE	DATA APPROVAZIONE CDA
0	-	Prima Emissione	30/08/2022
1	Aggiornato al DPR 81 / 2023	Aggiornamento	29/08/2023

1. Premessa

Il presente regolamento definisce le norme di gestione e organizzazione dei sistemi informativi (IT) dell' ASP AMBITO 9 .

2. Finalità

Le finalità del presente regolamento, in ordine di priorità, sono le seguenti:

1. Tutela del cittadino;
2. Tutela del patrimonio informativo dell'Ente;
3. Tutela dell'utilizzatore dei sistemi e delle reti di comunicazione;
4. Tutela dei sistemi informatici e delle reti di comunicazione;
5. Promozione della cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti di comunicazione;
6. Aumento della sensibilità rispetto ai rischi nell'uso dei sistemi e delle reti di comunicazione;
7. Chiarezza e divulgazione delle regole di comportamento, trasparenza delle procedure, gradualità nei controlli, proporzionalità e pertinenza degli interventi rispetto alla gravità dei sospetti e congruità delle reazioni.

2. Principi ispiratori

Come previsto dalle Raccomandazione del Consiglio dell'OCSE nella sua 1037ª sessione del 25 luglio 2002, relativamente sulla sicurezza dei sistemi e delle reti d'informazione, sono riportati i principi che hanno ispirato la redazione del presente regolamento e che ispirano la gestione dei Sistemi Informativi dell'ASP Ambito 9.

Sensibilizzazione
Le parti interessate devono essere sensibilizzate, formate e informate sui possibili rischi al fine di tutelare la sicurezza dei sistemi e delle reti di comunicazione.

Responsabilità
Le parti interessate sono (co-)responsabili della sicurezza dei sistemi e delle reti di comunicazione.

Risposta
Le parti interessate devono operare congiuntamente e tempestivamente al fine di prevenire, rilevare e rispondere agli incidenti di sicurezza.

Etica
Le parti interessate devono adoperarsi per elaborare e, successivamente, adottare delle pratiche esemplari nel pieno rispetto dei legittimi interessi delle altre parti.

Rispetto
Le parti interessate devono adottare tutte le misure di protezione possibile al fine di tutelare la dignità della persona, con particolare riferimento ai dati sensibili come previsto dalla vigente normativa privacy.

Applicazione della sicurezza
Le misure di protezione, tecniche e non tecniche, devono essere commisurate al valore delle informazioni memorizzate nei sistemi e veicolate nelle reti di comunicazione.

Interconnessione
La sempre più estesa interconnessione dei sistemi informativi, unita a livelli di complessità elevati, aumenta il rischio di compromissione della sicurezza delle informazioni. La sicurezza passa anche attraverso la consapevolezza della situazione attuale.

Politiche di sicurezza
La gestione della sicurezza deve essere dinamica e globale, per coprire tutti i livelli di attività delle parti interessate e tutti gli aspetti dei loro interventi.

Rivalutazione
Le parti interessate devono permanentemente riesaminare, rivalutare e modificare tutti gli aspetti della sicurezza per affrontare i nuovi rischi, in un'ottima di miglioramento continuo, secondo il ciclo di Deming (PDCA – *plan–do–check–act*).

3. Ambito di applicazione, perimetro

Il presente regolamento si applica a tutti gli utilizzatori di sistemi e dispositivi compresi nel perimetro dell'Ente, corrispondente alla massima estensione della rete di comunicazione privata fino al firewall di connessione con la rete pubblica, includendo anche i sistemi collegati via Virtual Private Network (VPN) e i sistemi posizionati in zone demilitarizzate (DMZ), in *hosting*, in *housing* o in cloud.

Si applica inoltre alla rete Wi-Fi dell'ASP.

Sono esclusi dal perimetro gli utilizzatori di sistemi e dispositivi collegati a reti isolate; sono inoltre esclusi dal perimetro gli utilizzatori di servizi pubblici forniti dall'Ente attraverso la rete Internet (ad esempio il sito web istituzionale).

4. Divieti e Obblighi

1. L'uso di tutti i dispositivi hardware dell'Ente è autorizzato per le sole finalità lavorative e professionali, nell'ambito della mansione e del profilo di autorizzazione previsto per l'utilizzatore. Qualsiasi altro utilizzo è vietato.

In deroga alle norme generali, al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali solo nel caso in cui questo eviti al dipendente di doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

2. È vietato modificare la posizione, la configurazione hardware e software, la modalità di collegamento alla rete dell'Ente, da parte dell'utilizzatore o di personale esterno, senza specifica autorizzazione.

Qualsiasi spostamento delle postazioni informatiche deve essere comunicata agli amministratori di sistema, per poterne consentire l'aggiornamento dell'inventario, il quale dovrà contenere le informazioni relative al titolare della risorsa e ufficio associato.

3. Non è consentito l'uso di software applicativi diversi da quelli distribuiti ufficialmente dall'Ente (ai sensi del D.Lgs. n. 518/1992 sulla tutela giuridica del software e Legge n. 248/2000 nuove norme di tutela del diritto d'autore).

4. È tassativamente vietato rivelare la propria password di accesso alla rete dell'Ente, ad uno degli applicativi o servizi disponibili (inclusi i siti regionali o ministeriali). Qualsiasi azione effettuata utilizzando la coppia "nome utente e password" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.

5. È vietato conservare nei sistemi e unità di memorizzazione assegnati, file, documenti, mail, immagini, video non legati alle finalità lavorative e professionali, in particolar modo di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso e/o discriminatorio.

6. È tassativamente vietata la navigazione in siti Internet non legati alle finalità lavorative e professionali, alla ricerca, allo studio e formazione. È vietato effettuare navigazione in siti web di contenuto osceno o violento, offensivo alla morale o alla pubblica decenza, oltraggioso, che incitino all'odio o alla discriminazione.

7. È tassativamente vietata la navigazione in siti Internet palesemente incompatibili con le finalità dell'Ente, che istighino a comportamenti illegali, che consentano o siano a rischio di diffusione di virus, cavalli di troia o di altri programmi il cui obiettivo sia la distruzione, alterazione, sabotaggio, intercettazione, hacking o pirateria informatica a danno dei computer di altri utenti interni o esterni al perimetro dell'Ente.

8. È vietato l'utilizzo dei social media, forum, chat-line, instant messaging, Voice over IP o video chat per finalità diverse da quelle professionali o di formazione.

9. È vietato l'invio di dati sensibili tramite posta elettronica convenzionale al di fuori del perimetro dell'Ente anche se il destinatario è un ente pubblico.

10. È vietato il trasporto al di fuori del perimetro dell'Ente di dispositivi di memorizzazione contenenti dati sensibili. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.

È obbligatorio utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti

11. E' obbligatorio attenersi alle norme che regolano l'utilizzo della posta elettronica di seguito elencate:

- Al dipendente, all'atto dell'assunzione, potrà essere assegnata una casella di posta elettronica aziendale che dovrà essere utilizzata per inviare e ricevere tutta la corrispondenza e gli allegati inerenti attività aziendali.
- L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.
- Il dipendente è responsabile del contenuto dei messaggi inviati.
- I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l' identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.
- E' vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.
- I dati trattati saranno accessibili agli amministratori di sistema per le attività di manutenzione ordinaria e straordinaria e potranno essere oggetto di trattamento da parte di colleghi e superiori per comprovate esigenze aziendali.
- Nei periodi di assenza del dipendente per ferie, congedi, malattia, ecc., la posta indirizzata alla sua mailbox aziendale potrà essere oggetto di temporaneo re indirizzamento nella mailbox di un collega, al fine di evitare che corrispondenza urgente o importante per l'azienda possa essere visionata in ritardo.
- Alla cessazione del rapporto, sull'indirizzo di posta elettronica aziendale sarà attivato un risponditore automatico che informerà i mittenti dell'avvenuta disattivazione della casella di posta elettronica con invito a trasmettere i messaggi ad altro indirizzo aziendale.
- Potrà essere assegnata una casella di posta elettronica aziendale anche a eventuali collaboratori esterni, previo accordo scritto circa obblighi e divieti sopra esplicitati

12. E' obbligatorio segnalare agli amministratori di sistema eventuali dimissioni o trasferimenti dei dipendenti, al fine di consentire l'eliminazione degli account non necessari

13. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

Al fine di garantirne i necessari profili di riservatezza, le comunicazioni - afferenti direttamente o indirettamente il servizio - non si svolgono di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

5. Controlli

L'amministrazione, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati.

Al fine di garantire la sicurezza del patrimonio informativo dell'Ente, le attività di navigazione Internet, di accesso alla rete dell'Ente, di inserimento, di modifica o cancellazione dei dati negli applicativi software, sono registrate in appositi file di log, adeguatamente protetti e consultabili solamente dagli Amministratori di Sistema nominati e dall'Autorità Giudiziaria.

Sono registrate ed archiviate le seguenti informazioni:

- giorno, ora, sistema utilizzato per l'accesso alla rete dell'Ente;
- indirizzi web consultati o dati inseriti, modificati, cancellati negli applicativi software;
- accessi alla rete Internet con tempi di connessione e quantità di dati scaricati.

Il tempo massimo previsto di conservazione delle registrazioni è di 6 mesi, a meno di diversa disposizione di legge o di provvedimento da parte dell'Autorità Giudiziaria.

6. Sanzioni

Il mancato rispetto o la violazione di quanto previsto dal presente Regolamento, tenuto conto del principio di proporzionalità, è perseguibile con l'irrogazione di provvedimenti disciplinari attraverso comunicazione dell'illecito al responsabile della struttura presso cui presta servizio il dipendente o all'ufficio per i procedimenti disciplinari secondo quanto stabilito nel Codice Disciplinare vigente.

7. Prescrizioni

L'attività di gestione e utilizzo degli strumenti informatici e dell'infrastruttura di rete segue le norme del presente Regolamento.

Il presente Regolamento è inviato come circolare a tutto il personale dipendente.

Gli utilizzatori interni ed esterni devono essere debitamente informati sul presente Regolamento prima di poter accedere ai sistemi o alla rete di comunicazione.

Periodicamente, per cambiamenti tecnologici, per esigenze di sicurezza informatica o per sopravvenute esigenze organizzative, si provvederà alla revisione del presente Regolamento.

Tutte le società/aziende pubbliche esterne che, mediante convenzione, usufruiscono dei servizi informatici dell'Ente sono tenute al rispetto del presente regolamento se utilizzano i servizi della rete (rete comunale o rete Wi-Fi dell'Ente) estendendone, di fatto, il perimetro. I Responsabili delle convenzioni dovranno garantire il rispetto di tale prescrizione.

Glossario

Amministratore di Sistema: figura professionale che si occupa della gestione e della manutenzione di un sistema di elaborazione e delle sue componenti.

Cloud: modalità di erogazione dei servizi informatici tramite infrastrutture informatiche esterne non gestite dal Comune di Jesi

DMZ:(zona demilitarizzate): segmento isolato di rete LAN raggiungibile sia dall'interno che dall'esterno (Internet).

Hosting (letteralmente ospitare): servizio che permette di pubblicare un sito o servizio web su macchine pubblicate in Internet di un fornitore.

Housing: servizio di affitto di spazi e infrastrutture per server di proprietà.

ICT: Tecnologie dell'informazione e della comunicazione.

Learning by doing (lett. imparare facendo): apprendimento informale effettuato durante le attività quotidiane.

Outsourcing: esternalizzazione dei processi.

Servizio Sviluppo Tecnologico: Servizio comunale per la gestione e lo sviluppo dei servizi Informatici

Switch e Router: dispositive di comunicazione di rete.

Troubleshooting: in un sistema complesso, la risoluzione di un malfunzionamento avviene attraverso l'esclusione progressiva di tutte le possibili cause.

VPN (Virtual Private Network): rete di telecomunicazioni privata, instaurata su un sistema di trasmissione pubblico e condiviso.

Bibliografia e sitografia

D. Lgs. 196/03 Codice in materia di protezione dei dati personali [testo consolidato vigente] integrato con le modifiche introdotte dal D.lgs 101/2018

Linee guida del Garante per posta elettronica e Internet - 1 marzo 2007 [doc. web n. 1387522]

Decreto Legislativo n. 151 del 14 settembre 2015, recante «Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014 n. 183» per la modifica art. 4 Statuto Lavoratori Legge 20 maggio 1970 n. 300.

Legge 18 marzo 2008, n. 48 “criminalità informatica”

Legge n. 38/06 “Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo pornografia anche a mezzo Internet”

D.Lgs. 81/08 “Testo Unico sulla salute e sicurezza sul lavoro”

Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 Doc. web [4129029] Garante privacy

Raccomandazione del Consiglio dell'OCSE nella sua 1037a sessione del 25 luglio 2002, relativamente sulla sicurezza dei sistemi e delle reti d'informazione

Regolamento Generale sulla Protezione dei Dati, regolamento (UE) n. 2016/679