Sistema Socio Sanitario
Regione Lombardia
ASST Santi Paolo e Carlo

Via A. di Rudinì,n.8 – 20142 MILANO
Tel. 02.8184.1 – Fax 02.8910875

Deliberazione n. 0002104 del 21/12/2018 - Atti U.O. S.C. Gestione Op. Area Territoriale

Oggetto: ADOZIONE DEL REGOLAMENTO PER LA SICUREZZA DEL TRATTAMENTO DEI DATI, DEL REGOLAMENTO PER LA GESTIONE DEL SISTEMA INFORMATIVO E DELLA PROCEDURA DI GESTIONE DEI DATA BREACH DELL'ASST SANTI PAOLO E CARLO

IL DIRETTORE S. C. "GESTIONE OPERATIVA AREA TERRITORIALE"

Premesso che, con DGR n. X/4473 del 10.12.2015, è stata costituita l' "Azienda Socio – Sanitaria Territoriale (ASST) Santi Paolo e Carlo" e che, pertanto, quest'ultima, ai sensi dell'art. 2, comma 8, lettera c), della Legge Regionale n. 23 dell'11.8.2015, a decorrere dall'1.1.2016. è subentrata nei rapporti giuridici attivi e passivi facenti capo alle A.O. San Paolo e A.O. San Carlo.

Vista la Deliberazione n. 1 dell'1.1.2016, esecutiva ai sensi di legge, avente ad oggetto "Presa d'atto della DGR n. X/4473 del 10.12.2015 "Attuazione L.R. 23/2015: Costituzione Azienda Socio – Sanitaria Territoriale (ASST) Santi Paolo e Carlo";

Richiamata la deliberazione n° 2 del 01/01/2016 avente per oggetto "*Insediamento del Direttore Generale dell'Azienda Socio Sanitaria Territoriale (ASST) Santi Paolo e Carlo*";

Visti:

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (d'ora innanzi GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- D. Lgs. 30 giugno 2003, n. 196, cosi come modificato dal D. Lgs. 10 Agosto 2018, n. 101: "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati e che abroga la direttiva 95/46/CE";

Richiamata la deliberazione n. 1301 del 22/08/2018 relativa all'adesione alla convenzione CONSIP SGI – lotto n. 4 per l'implementazione di una piattaforma SW dedicata (MUA), sviluppata in base alle caratteristiche peculiari dei processi amministrativi e dei sistemi informativi gestionali dell'A.S.S.T. Santi Paolo e Carlo, per la gestione nel tempo del registro dei trattamenti dei dati personali, della relativa analisi dei rischi e delle eventuali DPIA;

Richiamata altresì la deliberazione n. 814 del 30/5/2018 avente ad oggetto "Definizione del nuovo modello organizzativo privacy aziendale" laddove prevede, fra i compiti del Gruppo Privacy, la gestione dei Data Breach ivi compresa la stesura della comunicazione al garante e agli interessati qualora si rendessero necessarie;

Valutato che sono stati predisposti il "*Regolamento per la sicurezza del trattamento dei dati dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"* ed il "*Regolamento per la gestione del Sistema Informativo dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"* che indicano ai Responsabili

del trattamento (sia interni sia esterni) ed agli Autorizzati al trattamento le caratteristiche richieste ed implementate per la sicurezza dei dati (sia informatica che organizzativa) nonché le buone prassi da mantenere per la gestione dei documenti elettronici e cartacei coinvolti nei vari trattamenti aziendali, ed i comportamenti corretti (anche organizzativi) per la protezione delle informazioni trattate;

Dato atto che i suddetti Regolamenti sono stati trasmessi al SIA per la valutazione degli aspetti di propria competenza;

Considerato che la suddetta piattaforma MUA è dotata anche di un workflow per la gestione dei Data Breach, per l'invio delle comunicazioni e per la registrazione di tutte le attività connesse, compresa la visualizzazione e la stampa del registro dei Data Beach in modo da permetterne la visione al Garante e da garantire più in generale l'accountability di questo requisito imposto dal GDPR;

Valutato che è stata predisposta la procedura aziendale *"Procedura per la gestione dei Data Breach dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"* che norma i Responsabili dell'avvio della procedura di gestione dei Data Breach attraverso la piattaforma MUA, i responsabili della stesura del Verbale del Data Breacjh e della comunicazione al garante e agli interessati qualora si rendessero necessarie, nonché della chiusura del Data Breach;

Preso atto del decreto DGS n. 14513 del 10/10/2018 avente per oggetto: "Modifica e/o Integrazione dell'assegnazione a favore delle ATS, ASST, Fondazioni IRCCS, INRCA di Casatenovo, AREU e Agenzia dei Controlli delle risorse destinate al finanziamento di parte corrente del F.S.R. per l'esercizio 2018 a seguito procedure di assestamento;

Dato atto che il presente provvedimento non comporta oneri a carico del Bilancio Aziendale;

Ritenuto di approvare:

- il "*Regolamento per la sicurezza del trattamento dei dati dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"* allegato al presente atto, quale parte integrante e sostanziale (Allegato 1);
- il "*Regolamento per la gestione del Sistema Informativo dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"*, allegato al presente atto quale parte integrante e sostanziale (Allegato 2);
- la *"Procedura per la gestione dei Data Breach dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"*, allegato al presente atto quale parte integrante e sostanziale (Allegato 3);

Tutto ciò premesso, propone l'adozione della seguente deliberazione;

IL DIRETTORE GENERALE

Acquisiti i pareri favorevoli del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio-Sanitario

DELIBERA

Per i motivi di cui in premessa che qui si intendono integralmente trascritti:

1. di approvare il "*Regolamento per la sicurezza del trattamento dei dati dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"*, allegato al presente atto quale parte integrante e sostanziale (Allegato 1);

2. di approvare il "*Regolamento per la gestione del Sistema Informativo dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"*, allegato al presente atto quale parte integrante e sostanziale (Allegato 2);

3. di approvare la *"Procedura per la gestione dei Data Breach dell'Azienda Socio Sanitaria Territoriale Santi Paolo e Carlo"*, allegato al presente atto quale parte integrante e sostanziale (Allegato 3);

4. di adottare i suddetti regolamenti e la suddetta procedura aziendali a partire dal 20/12/2018;

5. di dare atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico di questa ASST;

6. di dare atto che il presente provvedimento è assunto su proposta del Direttore S.C. Gestione operativa Area territoriale dott. Piermauro Sala in qualità di Responsabile del Procedimento, che provvederà all'inoltro formale del provvedimento allegato;

7. di dare atto che il presente provvedimento deliberativo è immediatamente esecutivo, in quanto non soggetto a controllo di Giunta Regionale, verrà pubblicato sul sito internet Aziendale, ai sensi dell'art. 17 comma 6 L. R. n. 33/2009 e ss. mm. ii.

Documento firmato digitalmente da: Direttore Amministrativo Dott.ssa Maria Grazia Colombo, Direttore Sanitario Dott. Mauro Moreno, Direttore Socio Sanitario Dott.ssa Daniela Malnis, Direttore Generale Dott. Marco Salmoiraghi ai sensi delle norme vigenti D.P.R. n.513 del 10/11/1997, D.C.P.M. del 08/02/1999, D.P.R. n. 445 del 08/12/2000, D.L.G. Del 23/01/2002

Pratica trattata da: Gerarda Fiore

Dirigente/Responsabile proponente: PierMauro Sala

Il presente atto si compone di n. 42 pagine, di cui n. 38 pagine di allegati che costituiscono parte integrante e sostanziale.

REGOLAMENTO PER LA SICUREZZA DEL TRATTAMENTO DEI DATI

Sommario

1. Premessa 3
2. Oggetto e campo di applicazione del Regolamento 3
3. Politiche generali 4
4. Regole per gli accessi 5
5. Divieti 6
6. Politiche di “schermo pulito” 7
7. Supporti removibili 7
8. Dispositivi portatili 7
9. Utilizzo della rete Internet e dell’account di posta elettronica 8
10. Principali minacce 10
11. Comportamento da tener in caso di rilevazione anomalia o punto di debolezza del sistema informativo o indisponibilità dei dati 13
12. Utilizzo di fax, stampanti e fotocopiatrici, telefoni, tablet 13
13. Accesso ai dati trattati dall’Utente 14
14. Indicazioni per il trattamento dei dati senza l’ausilio di strumenti elettronici 14
15. Controlli 15
15.1. Sistemi di controllo graduali 15
16. Sanzioni 16
17. Entrata in vigore, riesame e aggiornamento 16

1. Premessa

La sicurezza delle informazioni costituisce un valore imprescindibile per l'ASST Santi Paolo e Carlo e per i suoi lavoratori, in particolare nell'ambito della postazione di lavoro e dei sistemi informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, l'ASST Santi Paolo e Carlo ha adottato il presente "***Regolamento per la sicurezza del trattamento dei dati***" (d'ora in avanti "Regolamento"), volto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati (personali e non), dei documenti e delle apparecchiature elettronico informatiche e volto ad adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi.

Lo scopo del presente Regolamento è quello di indicare i limiti entro cui i fruitori possono legittimamente usare gli strumenti elettronici messi a disposizione dall'ASST Santi Paolo e Carlo al fine di uno svolgimento proficuo e più agevole della propria attività (personal computer, smartphone, tablet, etc.), evitando di esporre sé stessi e/o l'ASST Santi Paolo e Carlo a gravi conseguenze che, in taluni casi, determinano ingenti sanzioni pecuniarie e, nei casi più gravi, possono investire il diritto penale.

Il Regolamento è stato implementato per tutelare la sicurezza dei sistemi informativi dell'ASST Santi Paolo e Carlo, assicurando la disponibilità delle risorse informative e dei dati, l'integrità dei sistemi e dei dati e la riservatezza delle informazioni.

Il Regolamento, oltre a dettare una disciplina per l'utilizzo degli strumenti aziendali, è da considerarsi uno **strumento di formazione e sensibilizzazione** per il personale nell'ambito degli obiettivi e delle Politiche di sicurezza delle informazioni adottate dall'ASST Santi Paolo e Carlo.

L'ASST Santi Paolo e Carlo ha ritenuto inoltre di porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità.

A tal fine il presente strumento regolamenta l'utilizzo degli strumenti elettronici atti a rendere la prestazione lavorativa in conformità alle prescrizioni dell'art. 4, comma 2, Legge 300/1970 (come modificato dall'art. 23 del D. Lgs. 151/2015), della Deliberazione n. 13 del 01/03/2007 del Garante per la protezione dei dati personali "Linee guida per la posta elettronica ed internet", del General Data Protection Regulation - GDPR (Regolamento 679/2016/UE) e tutte le sue norme attuative vigenti.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni eventualmente già fornite agli incaricati ed agli specifici responsabili designati. Esse inoltre integrano le eventuali informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

2. Oggetto e campo di applicazione del Regolamento

L'oggetto del Regolamento è:

- disciplinare le modalità di utilizzo di qualsiasi dotazione per il trattamento dei dati messa a disposizione dall'ASST Santi Paolo e Carlo, sia all'interno sia all'esterno delle sedi di lavoro, ivi compresi eventuali siti di telelavoro, atta a rendere la prestazione lavorativa;
- elencare i doveri che ciascun utilizzatore è tenuto ad osservare.

L'utilizzo delle risorse e dei servizi è subordinato al rispetto da parte degli utilizzatori del presente Regolamento, oltre che delle norme civili, penali e amministrative applicabili.

Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, a tutti i collaboratori dell'ASST Santi Paolo e Carlo a prescindere dal rapporto contrattuale con la stessa intrattenuto e a chiunque abbia in dotazione, anche temporaneamente, risorse informatiche e telematiche di proprietà dell'ASST Santi Paolo e Carlo o ad essa affidate. Tali soggetti, nell'ambito del presente Regolamento, sono indicati nel seguito anche come "Utente", "Utilizzatore" o "Incaricato".

Il presente Regolamento si applica a qualsiasi dotazione ICT intesa come risorsa informatica e/o telematica (a titolo esemplificativo e non esaustivo computer, notebook, server, software, rete, utenza, file, cartella di rete, internet key, telefono, tablet, smartphone, modem, ecc..), di seguito indicata anche come strumento elettronico, messa a disposizione dall'ASST Santi Paolo e Carlo all'Utente per rendere la prestazione lavorativa.

3. Politiche generali

Tutti gli strumenti elettronici affidati all'Utente sono da considerarsi uno **strumento di lavoro**. Possono essere utilizzati solo per fini professionali (in relazione alle mansioni assegnate) e non a fini personali. Quindi ogni utilizzo non inerente l'attività lavorativa è vietato. La deroga alla presente condizione è consentita solo in caso di specifica approvazione da parte del Titolare o suo delegato.

Tutti gli strumenti elettronici affidati all'Utente non possono essere utilizzati per scopi illeciti e devono essere custoditi con cura ed in modo appropriato evitando ogni possibile forma di danneggiamento.

Gli strumenti elettronici devono essere spenti al termine della propria sessione lavorativa giornaliera, in caso di assenze prolungate dall'ufficio o in caso di loro inutilizzo. Qualora l'elaboratore sia utilizzato da più incaricati, alla conclusione dei lavori è necessario disconnettere il proprio account dal sistema. Prima di effettuare la disconnessione chiudere i programmi rimasti eventualmente aperti. In questo modo la persona che utilizzerà il personal computer in seguito potrà comunque effettuare la procedura di autenticazione. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Si fa presente che tutti i dischi o altre unità di memorizzazione locali potrebbero non essere soggetti a salvataggio da parte del sistema informatico dell'ASST Santi Paolo e Carlo. Pertanto gli Utenti sono tenuti a memorizzare la documentazione lavorativa esclusivamente sui server dell'ASST Santi Paolo e Carlo.

È indispensabile che nessun dato personale degli Utenti non inerente l'attività lavorativa sia presente sulle risorse informatiche dell'ASST Santi Paolo e Carlo neppure provvisoriamente.

Per i PC non appartenenti alla rete dell'ASST Santi Paolo e Carlo, non avendo accesso diretto ai server e di conseguenza ai salvataggi periodici, i dati devono essere conservati sul disco locale e periodicamente salvati secondo le istruzioni impartite dall'Amministratore di sistema o dal Responsabile IT.

Ogni Utente è responsabile della propria postazione informatica, della propria casella di posta elettronica e del contenuto dei messaggi da essa inviati. È inoltre responsabile della segretezza delle credenziali di accesso alla rete e ai software al cui utilizzo è stato autorizzato.

Ogni Utente è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione o perdita accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Utenti sono tenuti a mantenersi aggiornati, prendendo visione delle eventuali disposizioni emanate e divulgate tramite pubblicazione in area dedicata nella rete informatica dell'ASST Santi Paolo e Carlo, tramite posta elettronica o tramite altro strumento cartaceo (avviso, disposizione, regolamento, ecc.).

Resta inteso che tutte le risorse informative, sia in termini di strumenti che in termini di dati, rimangono di proprietà dell'ASST Santi Paolo e Carlo e che l'Utente è tenuto a restituire la totalità delle risorse utilizzate nel momento in cui dovesse cessare il rapporto con l'ASST Santi Paolo e Carlo o nel caso in cui gli venisse richiesto da quest'ultima.

Gli Utenti sono tenuti a dare tempestiva comunicazione, preferibilmente in forma scritta, di qualsiasi anomalia relativa al sistema informativo aziendale al Titolare o suo delegato affinché la stessa venga valutata dal personale all'uopo incaricato e gestita nel rispetto delle procedure di sicurezza dell'ASST Santi Paolo e Carlo.

4. Regole per gli accessi

L'accesso alla rete informatica dell'ASST Santi Paolo e Carlo e l'utilizzo degli strumenti elettronici dati in affidamento all'Utente è consentito solo attraverso specifiche credenziali di autenticazione, che consistono in un codice per l'identificazione (username) dell'incaricato associato a una parola chiave (password) riservata conosciuta solamente dal medesimo (in alternativa in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato).

Gli accessi ed i permessi degli Utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Ne consegue che gli Utenti possono effettuare esclusivamente i trattamenti di dati personali che rientrano nel proprio ambito lavorativo e per i quali hanno ricevuto specifico incarico. Tali trattamenti devono essere effettuati esclusivamente in conformità alle finalità previste e alle informazioni comunicate agli Interessati.

L'Utente è tenuto a modificare la parola chiave (password) assegnatagli al primo accesso tenendo conto di quanto segue:

- la password deve essere complessa (a titolo esemplificativo: deve contenere lettere e numeri e/o simboli, minimo 8 caratteri, minuscole, Maiuscole);
- la password non deve essere agevolmente riconducibile all'Utente (a titolo esemplificativo non deve essere identica allo username, non deve essere la data di nascita ecc.);
- la sequenza delle password non può essere la medesima di quelle precedenti;
-
- le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Utente, in qualità di incaricato, l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto;
- è vietato affidare al sistema operativo la memorizzazione automatica delle password e l'Utente è tenuto a digitare la password ad ogni accesso;
- è attivo un sistema di blocco delle credenziali di autenticazione in caso di errato inserimento delle stesse per un numero di volte consecutive superiore ad una soglia predefinita, comunicata dal sistema;
- il sistema richiede la modifica della parola chiave (password) ogni sei mesi e, in caso di trattamento di dati sensibili e/o giudiziari, ogni tre mesi;

- sul sistema sono impostati time-out di inattività e screen-saver che, in caso di inattività sullo strumento di durata superiore ad un lasso temporale predefinito, richiedono all'Utente il re-inserimento delle proprie credenziali di autenticazione.

Il codice di identificazione non deve essere comunicato ad alcuno e deve essere custodito dall'Utente con la massima diligenza e non divulgato, seguendo scrupolosamente le indicazioni impartite dall'ASST Santi Paolo e Carlo.

È assolutamente proibito accedere alla rete e ai programmi con un codice di identificazione Utente diverso da quello assegnato.

L'Utente è tenuto ad avvisare prontamente l'ufficio competente al riguardo nell'ipotesi di smarrimento dei dati di accesso.

In caso di prolungata assenza o impedimento di un Utente che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile IT (o l'Amministratore di sistema o l'incaricato alla custodia delle credenziali, se designati), su indicazione della Direzione, al fine di assicurare la disponibilità dei dati e/o degli strumenti elettronici, potrà resettare la componente riservata della credenziale di autenticazione, per consentire l'accesso ad un altro Utente indicato dalla Direzione.

Per le utenze di Administrator si utilizzerà la procedura della busta chiusa, che prevede la comunicazione delle proprie credenziali privilegiate di autenticazione solo ed esclusivamente al soggetto incaricato alla custodia delle credenziali, tramite documento sottoscritto dall'Utente, sigillato in busta chiusa e consegnato *brevi manu* al soggetto su indicato.

L'Utente, terminato il periodo di assenza o impedimento, sarà immediatamente informato in merito all'intervento effettuato e dovrà modificare la propria componente riservata della credenziale di autenticazione.

5. Divieti

È vietato, salvo preventiva ed espressa autorizzazione dell'ASST Santi Paolo e Carlo:

- l'uso di programmi diversi da quelli ufficialmente installati;
- installare, modificare e aggiornare i software autonomamente, se non inclusi nell'elenco software autorizzati;
- modificare le caratteristiche impostate sul proprio personal computer e procedere ad installare dispositivi di memorizzazione, comunicazione o altro;
- utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o eliminare il contenuto di comunicazioni e/o documenti informatici;
- utilizzare e conservare sul sistema informatico dell'ASST Santi Paolo e Carlo di file non attinenti l'attività lavorativa;
- violare l'integrità di dati personali;
- compromettere l'integrità dei sistemi;
- saturare le risorse in misura tale da compromettere l'efficienza del sistema informativo dell'ASST Santi Paolo e Carlo;
- compiere atti di criminalità informatica;
- consentire l'accesso alla rete e/o condividere la rete con soggetti non autorizzati;
- usare false identità;
- violare la sicurezza, trasferire, comunicare, diffondere, intercettare, accedere a dati per i quali non si ha specifica autorizzazione;
- collegare alla rete aziendale computer personali o computer non assegnati dall'ASST Santi Paolo e Carlo;

- accedere ad aree, chiaramente definite e segnalate dall'ASST Santi Paolo e Carlo, che contengono informazioni sensibili o critiche e strutture di elaborazione delle informazioni, se non specificatamente autorizzati;
- consentire l'accesso alle aree in cui si esegue il trattamento dei dati a personale esterno non autorizzato;
- trasferire all'esterno del sito, anche fisicamente, le apparecchiature, informazioni o software senza preventiva autorizzazione.

Si evidenzia che alcune delle violazioni di cui sopra sono sanzionabili anche penalmente.

6. Politiche di "schermo pulito"

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l'Utente segua delle politiche di "schermo pulito". In particolare è fondamentale che presti particolare attenzione alle schermate a video contenenti informazioni non pubbliche. È quindi opportuno che tali schermate siano mantenute solo per il tempo strettamente necessario.

7. Supporti removibili

I supporti rimovibili contenenti dati personali, se non utilizzati, devono essere distrutti o resi inutilizzabili prima di procedere al loro smaltimento. Tali supporti possono essere utilizzati da altri Incaricati se le informazioni precedentemente in essi contenute sono inintelligibili e tecnicamente in alcun modo ricostruibili.

In caso di utilizzo di supporti di origine esterna l'Utente deve procedere all'esecuzione di una scansione anti-malware degli stessi e deve disattivare l'esecuzione automatica dei contenuti.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli Utenti adeguatamente custoditi in locali o in soluzioni di stoccaggio ad accesso ristretto e controllato (a titolo esemplificativo, armadi o cassetti chiusi a chiave, casseforti e simili).

L'uso di supporti esterni deve essere limitato a quelli necessari per le attività dell'ASST Santi Paolo e Carlo.

È vietato l'utilizzo di supporti rimovibili personali.

L'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

8. Dispositivi portatili

L'Utente è responsabile dei dispositivi portatili assegnatogli dall'ASST Santi Paolo e Carlo e deve custodirli con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

I dispositivi portatili, proprio per le loro intrinseche caratteristiche, sono più vulnerabili dei dispositivi fissi. Per tale motivo, oltre alle politiche adottate per gli strumenti informatici fissi, occorrono accorgimenti aggiuntivi. Quindi, al fine di minimizzare il rischio associato al furto, all'uso fraudolento e all'accesso di persone non autorizzate alle informazioni presenti sui dispositivi, dovrà essere valutata con il Responsabile IT, in base al tipo di trattamenti eseguiti con tali strumenti, l'opportunità di dotare i dispositivi portatili di un sistema di cifratura dei dati contenuti nell'hard disk, affinché, qualora venga superato il meccanismo di autenticazione dell'accesso, comunque i dati risultino assolutamente indecifrabili.

I dispositivi portatili, al fine di garantire il controllo, l'aggiornamento e l'allineamento alle politiche di sicurezza dell'ASST Santi Paolo e Carlo, devono essere periodicamente connessi, direttamente o tramite connessione protetta, alla rete dell'ASST Santi Paolo e Carlo, per la durata necessaria.

9. Utilizzo della rete Internet e dell'account di posta elettronica

La navigazione in Internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione. L'uso della posta elettronica e della rete Internet, nelle sue numerose funzionalità, è consentito esclusivamente per gli scopi attinenti alle mansioni lavorative assegnate, salvo preventiva ed espressa autorizzazione dell'ASST Santi Paolo e Carlo.

I dati che vengono inviati mediante il sistema di posta elettronica dell'ASST Santi Paolo e Carlo sono di proprietà della stessa.

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica assegnate e/o messe a disposizione dall' ASST Santi Paolo e Carlo per motivi diversi da quelli strettamente legati all'attività lavorativa e per motivi non attinenti allo svolgimento di mansioni lavorative assegnate.

La "personalizzazione" dell'indirizzo di posta elettronica, ovvero la possibilità che esso contenga riferimenti al nome e cognome dell'utente, non comporta il fatto che la stessa venga considerata "privata", in quanto si tratta comunque di uno strumento di esclusiva proprietà dell'azienda / dell'Ente, messo a disposizione di dipendenti e collaboratori a vario titolo al solo fine dello svolgimento delle proprie mansioni lavorative.

La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Prima di aprire i file allegati ai messaggi di posta elettronica, è necessario identificare il mittente e porre particolare attenzione alla tipologia del file stesso, in caso in cui non si conosca il mittente è consigliabile cancellare tutto, messaggio ed allegato, o sottoporlo a verifica da parte del servizio IT onde evitare attacchi informatici. E' comunque sconsigliato eseguire file allegati ai messaggi di posta elettronica.

Sarà comunque consentito accedere alla casella di posta elettronica dell'Utente per ogni ipotesi in cui si renda necessario per le esigenze dell'ASST Santi Paolo e Carlo, tramite apposita procedura.

Al fine di ribadire agli interlocutori la natura della casella di posta elettronica assegnata dall'ASST Santi Paolo e Carlo, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.

Inserire nei messaggi di posta elettronica la seguente dicitura:

> *"Questa comunicazione e ogni eventuale file allegato sono ad uso esclusivo del destinatario e potrebbero contenere informazioni riservate. Se non siete l'effettivo destinatario, o un dipendente, o la persona responsabile della consegna della comunicazione, e se l'aveste ricevuta per errore, ci scusiamo per l'accaduto e Vi invitiamo cortesemente a darcene notizia e a distruggerla. Il messaggio ed eventuali file allegati non hanno natura personale e le eventuali risposte alla presente potranno essere conosciute da più soggetti e unità operative all'interno dell'ASST Santi Paolo e Carlo, che a vario titolo abbiano interesse ad assolvere le specifiche richieste o esigenze oggetto della comunicazione. Qualsiasi modifica o distribuzione a terzi è assolutamente vietata. Vi ricordiamo, inoltre, che la comunicazione, la diffusione, l'utilizzo e/o la conservazione dei dati ricevuti per errore, costituiscono violazioni alle disposizioni del Regolamento Generale sulla protezione dei dati personali 679/2016 dell'Unione Europea e sono sanzionabili ai sensi dell'art. 616 del Codice Penale."*

In caso di violazione o inadempimento di quanto riportato al presente paragrafo in merito all'utilizzo della posta elettronica, l'ASST Santi Paolo e Carlo procederà ad impedire all'Utente la possibilità di collegamento alla casella di posta elettronica assegnata e si procederà per

l'eventuale accertamento di responsabilità disciplinari, in caso di personale dipendente, o contrattuali in caso di professionisti e/o collaboratori.

L'ASST Santi Paolo e Carlo mette a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto.

È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati allo svolgimento delle mansioni lavorative assegnate, salvo preventiva ed espressa autorizzazione dell'ASST Santi Paolo e Carlo.

È assolutamente proibita la navigazione in Internet qualora il contenuto dei siti sia di natura oltraggiosa e discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Il sistema di sicurezza adottato e interposto tra la rete dell'ASST Santi Paolo e Carlo e la rete Internet potrà impedire l'accesso a siti web indesiderati, attraverso la valutazione del contenuto o per l'appartenenza ad una "black list".

Per ridurre il rischio di attacchi informatici durante la navigazione, posizionare il cursore del mouse sul link interessato, osservandone il percorso sulla barra del browser: se è un file eseguibile potrebbe trattarsi di un programma malevolo (ad esempio di un programma che potrebbe collegare l'Utente a un altro indirizzo internet, non sicuro).

Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto al personale del Servizio IT.

L'Utente è direttamente e totalmente responsabile dell'uso di Internet, delle informazioni che immette, delle modalità con cui opera, dei siti web o pagine internet ai quali abbia stabilito collegamento tramite link.

Qualora vengano attivati eventuali controlli da parte dell'ASST Santi Paolo e Carlo, tenuto conto degli strumenti elettronici installati, avverranno come di seguito indicato:

- gli apparati in uso, (ad esempio tramite un sistema proxy server) tracceranno in modo anonimo la navigazione effettuata dagli utenti in merito ai siti rilevati;
- tale tracciamento potrà essere visualizzato solo dall'Amministratore di sistema;
- nel caso di un sospetto illecito, l'Amministratore di sistema potrà abilitare, previa comunicazione agli utenti, la tracciatura degli accessi con associazione utente –sito visitato;
- il controllo potrà essere effettuato per un massimo di 6 mesi, tempo massimo di conservazione anche dei log di navigazione.

L'ASST Santi Paolo e Carlo periodicamente potrà effettuare controlli a campione sugli accessi internet effettuati dai dipendenti/collaboratori stessi.

Si rende noto che l'ASST Santi Paolo e Carlo è autorizzata al trattamento in forma anonima, tale da precludere l'immediata identificazione degli utenti, dei dati relativi al "traffico" internet. I file di LOG verranno conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

Verranno prolungati i tempi di conservazione (limitatamente comunque alle sole informazioni indispensabili per perseguire finalità preventivamente determinate) solo in caso di:

- esigenze tecniche o di sicurezza del tutto particolari;

- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o conservare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Il controllo anonimo potrebbe concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite.

Si ribadisce che i controlli rispettano i principi di pertinenza e di non eccedenza.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori etc.) tanto della rete Internet che della posta elettronica. Nell'esercizio del potere di controllo l'ASST Santi Paolo e Carlo si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

10. Principali minacce

Al fine di sensibilizzare gli utenti ad un uso diligente delle risorse messe a disposizione dall'ASST Santi Paolo e Carlo, vengono indicate di seguito alcune minacce che rappresentano una fonte di rischio per l'intero sistema informativo:

Malware

Nella sicurezza informatica il termine malware indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito.

Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno.

Si distinguono molte categorie di malware, anche se spesso questi programmi sono composti di più parti interdipendenti e rientrano pertanto in più di una classe. Vista inoltre la rapida evoluzione in questo campo, la classificazione presentata di seguito non è da ritenersi esaustiva.

Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.

Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.

CryptoLocker: una forma di ransomware infettante i sistemi Windows e che consiste nel criptare i dati della vittima, richiedendo un pagamento per la decriptazione. Cryptolocker generalmente si diffonde come allegato di posta elettronica apparentemente lecito e inoffensivo che sembra provenire da mittenti legittimi.

Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un Worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.

Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan.

Scareware: sono così chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, chiamati in gergo rogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta spacciati anche a pagamento.

Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.

Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

Batch: i Batch sono i cosiddetti "virus amatoriali". Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altri comandi dannosi) dell'utente a cui viene mandato il file. Non si apre automaticamente, deve essere l'utente ad aprirlo, perciò dato che l'antivirus non rileva i file Batch come pericolosi è sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolosità. Bisogna però anche dire che esistono modi per camuffare i Batch e farli sembrare dei file exe, aumentandone anche il peso per sedare ogni sospetto. L'utilizzo di questo particolare "malware" è spesso ricorrente nel Cyberbullismo.

Keylogger: i Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del Keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i Keylogger vengono installati sul computer dai trojan o dai Worm, in altri casi invece il Keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente.

Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.

Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.

Zip Bomb: è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a occupare tutto lo spazio su disco rigido.

Nell'uso comune il termine virus viene utilizzato come sinonimo di malware e l'equivoco viene alimentato dal fatto che gli antivirus permettono di rilevare e rimuovere anche altre categorie di software maligno oltre ai virus propriamente detti.

Intercettazioni delle comunicazioni: possono comportare l'accesso non autorizzato alle banche dati per consultazione e copia di dati personali da parte di persone non autorizzate.

Attacchi alle password: questi attacchi effettuati in varia forma sono dei tentativi per venire a conoscenza e quindi rubare le password degli utenti, di programmi e di accesso a siti Internet. Alcuni esempi sono i seguenti:

Brute Force: un apposito programma prova tutte le possibili combinazioni di chiavi per decrittare il file protetto.

Attacco a Dizionario: prova lunghissimi elenchi di parole, nomi e sigle di uso comune in una data lingua.

Attacco all'Algoritmo: prevede la possibilità di intervenire su particolari debolezze matematiche o computazionali dell'algoritmo utilizzato.

Password Sniffing: ruba la password - sniff - con qualche trucco, carpendola con un inganno ad esempio fingendosi responsabili di un servizio assistenza clienti o della sicurezza.

Crimini informatici: i sistemi informatici potrebbero essere utilizzati per compiere crimini informatici con implicazioni di tipo civile e penale (spamming, tentativi di intrusione, trattamento di testi o immagini proibite, violazione della corrispondenza, scaricamento di software o file non autorizzato o coperti da diritto d'autore, etc.).

Danni all'hardware: l'elemento più delicato dell'elaboratore è il disco fisso. Se si dovesse danneggiare, a meno di ricorrere a pratiche costosissime sviluppate da centri specializzati, tutti i dati andrebbero persi. Quindi è fondamentale la centralizzazione di tutti i dati sul server.

Usurpazione di identità: al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione e potrebbe scaricare un software maligno da un sito web che si fa passare per fonte affidabile per cui si potrebbero anche rivelare informazioni riservate alla persona sbagliata.

IP spoofing: l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Spamming: saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori messaggi.

Incidenti ambientali e eventi imprevisti: calamità naturali (tempeste, inondazioni, incendi e terremoti); guasti dell'hardware o del software dei componenti o dei programmi utilizzati; errore umano dell'operatore (compresi i fornitori di servizi) o dell'utente (ad esempio problemi di gestione della rete, installazione errata del software).

11. Comportamento da tener in caso di rilevazione anomalia o punto di debolezza del sistema informativo o indisponibilità dei dati

In caso di rilevazione di un'anomalia o punto di debolezza del sistema informativo, soprattutto se impatta o può potenzialmente impattare sulla sicurezza dei dati personali intesa come integrità, disponibilità e riservatezza, l'Utente è tenuto a darne tempestiva comunicazione, possibilmente scritta, al Responsabile opportunamente individuato. L'utente deve inoltre collaborare attivamente con quest'ultimo, in base alle indicazioni ricevute, per la tempestiva risoluzione e per la verifica del ripristino delle condizioni di normalità.

In caso si verifichi una violazione dei dati personali (Data Breach), ossia una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati è necessario darne immediata comunicazione al Responsabile del Trattamento o al Responsabile della Protezione dei Dati - RPD o al Titolare, affinché possano attivare le procedure di notifica previste dalla legge così come stabilite e dettagliate dalla *Procedura di Gestione del Data Breach*.

Il Responsabile della Protezione dei dati-RPD/Data Protection Officer-DPO individuato dall'ASST Santi Paolo e Carlo è il seguente soggetto:

RPD/DPO	**E-mail**	**Telefono**
PERINATI PIERLUIGI MARIO	rpd@asst-santipaolocarlo.it	02.8184.2119

ll Data Protection Officer è reperibile presso la sede del Presidio San Carlo in Via Pio II n. 3. In caso di istanze/comunicazione scritte da inviarsi in modalità digitale il Responsabile della Protezione dei dati - RPD può essere contattato utilizzando i recapiti istituzionali (rpd@asst-santipaolocarlo.it) indicati sul sito web dell'Ente.

12. Utilizzo di fax, stampanti e fotocopiatrici, telefoni, tablet

Il telefono o qualsiasi strumento di telefonia o connettività mobile affidato all'Utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.

L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale o di qualsiasi strumento di telefonia o connettività mobile affidato all'Utente è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità alle istruzioni al riguardo impartite dall'ASST Santi Paolo e Carlo.

È vietato l'utilizzo dei fax dell'ASST Santi Paolo e Carlo per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte dell'ASST Santi Paolo e Carlo.

Inserire a piè di pagina dei fax inviati la seguente dicitura:

> *"Questo messaggio fax è ad uso esclusivo del soggetto cui è indirizzato, e potrebbe contenere informazioni riservate. Se aveste ricevuto questo fax per errore, ci scusiamo per l'accaduto e Vi invitiamo cortesemente a darcene notizia e a distruggere il messaggio ricevuto. Vi ricordiamo, inoltre, che la comunicazione, la diffusione, l'utilizzo e/o la conservazione dei dati ricevuti per errore, costituiscono violazioni alle disposizioni del Regolamento Generale sulla protezione dei dati personali 679/2016 dell'Unione Europea e sono sanzionabili ai sensi dell'art. 616 del Codice Penale."*

È vietato l'utilizzo delle fotocopiatrici e delle stampanti dell'ASST Santi Paolo e Carlo per fini personali, salvo preventiva ed esplicita autorizzazione di quest'ultima.

13. Accesso ai dati trattati dall'Utente

È facoltà dell'ASST Santi Paolo e Carlo, tramite il personale incaricato della gestione del sistema informatico o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla *privacy*, a tutti gli strumenti informatici dell'ASST Santi Paolo e Carlo e ai documenti ivi contenuti. Le informazioni raccolte mediante tali operazioni di accesso, sulla base del presente regolamento che funge anche da strumento informativo, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro ai sensi dell'art. 4, comma 3, Legge 300/1970 (come modificato dal D. Lgs. 151/2015).

14. Indicazioni per il trattamento dei dati senza l'ausilio di strumenti elettronici

Al fine di ridurre il rischio di accesso non autorizzato ad informazioni aziendali, è necessario che l'Utente segua delle politiche di "scrivania pulita". Con tali termini si intende che l'Utente presti particolare attenzione a materiale cartaceo e dispositivi di memoria rimovibili.

Di conseguenza gli atti e i documenti contenenti dati personali comuni identificativi devono essere conservati nel rispetto di quanto segue:

- conservazione in archivi ad accesso selezionato;
- particolare attenzione posta alle stampe che, a volte, possono essere dimenticate sulle stampanti o ritirate dopo un tempo piuttosto lungo, lasciandole così incustodite e a disposizione di chiunque;
- l'Incaricato in caso di assenza - anche momentanea - dall'ufficio provvede a riporre la documentazione negli archivi;
- al termine del trattamento la documentazione deve essere restituita o distrutta se non sussiste l'esigenza di conservazione;
- la distruzione della documentazione deve essere effettuata in modo che non vi sia la possibilità di recupero e/o consultazione, e quindi sono da evitare cestini o contenitori per il riciclaggio della carta senza prima essersi assicurati dell'impossibilità del recupero del contenuto della documentazione;
- nel caso gli archivi contenenti dati personali siano ubicati in zona con accesso al pubblico, sono previsti armadi o contenitori muniti di serratura e sono predisposte "barriere" o distanze "di sicurezza" tali da impedire che soggetti non autorizzati possano visionare documenti durante il trattamento da parte degli Incaricati;
- non trasferire i documenti contenenti dati personali al di fuori dei locali preposti alla loro conservazione, se non in casi del tutto eccezionali.

In aggiunta, in caso di trattamento di dati personali sensibili e/o giudiziari o comunque critici:

- la documentazione deve essere conservata in luoghi ad accesso controllato e selezionato e custodita in archivi muniti di serratura (locali e armadi chiusi a chiave - anche elettronica, cassetti chiusi a chiave, casseforti, etc.);
- la documentazione contenente dati personali sensibili e/o giudiziari deve essere conservata separatamente rispetto alla documentazione cartacea contenente dati personali comuni identificativi.

In caso di utilizzo di fax e posta tradizionale, l'Utente deve inoltre osservare le seguenti indicazioni:

- per la gestione dei fax e le comunicazioni mediante posta tradizionale, possono essere individuati uno o più soggetti Incaricati al trattamento dei suddetti documenti;
- è cura dell'Incaricato smistare e consegnare i documenti alle persone o agli uffici competenti, evitando che il trattamento venga effettuato da persone non autorizzate;
- i documenti ricevuti per errore devono essere distrutti o restituiti al mittente senza essere diffusi e/o utilizzati.

15. Controlli

Al fine di verificare il corretto utilizzo degli strumenti come da prescrizioni esplicitate nel presente paragrafo potranno essere svolti dei controlli sia "remoti" (attraverso sistemi software all'uopo deputati) che "fisici" presso le singole postazioni o i singoli strumenti.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

I controlli saranno svolti in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema, sia per verificare il corretto utilizzo da parte degli utenti (dipendenti, collaboratori etc.). Nell'esercizio del potere di controllo l'ASST Santi Paolo e Carlo si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo.

Il personale tecnico specificatamente incaricato è autorizzato a compiere interventi nel sistema informatico dell'ASST Santi Paolo e Carlo ed ha la facoltà di collegarsi alle singole postazioni di lavoro al fine di garantire l'assistenza tecnica, la normale attività operativa e la sicurezza e salvaguardia del sistema stesso.

Il personale incaricato della gestione del sistema informatico può in qualunque momento procedere alla rimozione di ogni file o applicazioni installati in violazione delle prescrizioni di cui al presente regolamento.

Il personale incaricato della gestione del sistema informatico può in qualunque momento eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

15.1. Sistemi di controllo graduali

L'ASST Santi Paolo e Carlo informa circa la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo degli strumenti di cui al presente Regolamento nel rispetto dei criteri e dei principi stabiliti dal Garante per la protezione dei dati personali (provvedimento n. 13 del 01/03/07) e di valutare conseguentemente gli usi scorretti che, oltre ad esporre l'ASST Santi Paolo e Carlo stessa a rischi, tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile.

I controlli sull'uso degli strumenti informatici/telefonici tuttavia garantiranno tanto il diritto di proteggere la propria ASST Santi Paolo e Carlo, essendo strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori (legge n. 300/1970) e dal General Data Protection Regulation - GDPR (Regolamento 679/2016/UE).

Il Regolamento, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stato redatto tenendo opportunamente conto altresì delle disposizioni contenute nella Legge. n. 300/1970 in tema di provvedimenti disciplinari.

Nel rispetto della normativa in tema di protezione dei dati personali, l'attività di controllo espletata dall'ASST Santi Paolo e Carlo garantisce il rispetto dei principi fondamentali di "proporzionalità", i diritti e le libertà fondamentali, nonché la dignità dell'interessato e soprattutto prevede la fornitura di un'adeguata e preventiva informativa.

Si comunica pertanto che in caso di anomalie, il personale incaricato dalla Direzione potrà effettuare controlli anonimi, che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area / settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente C.C.N.L. applicabile, nonché con tutte le azioni civili e penali consentite anche nei confronti di collaboratori e professionisti.

17. Entrata in vigore, riesame e aggiornamento

Il presente regolamento è in vigore a partire dal 20/12/2018.

Il Regolamento viene riesaminato ed eventualmente aggiornato con cadenza periodica annuale o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

REGOLAMENTO PER LA GESTIONE DEL SISTEMA INFORMATIVO

Sommario

1. Oggetto e campo di applicazione del Regolamento 3
2. Politiche generali 4
3. Accessi logici 4
3.1. Procedura da adottare in caso di in caso di prolungata assenza o impedimento di un utente 6
4. Installazione, cambiamento e aggiornamento di apparecchiature informatiche 6
4.1. Messa in linea di server 7
4.2. Installazione e aggiornamento software e patch 7
5. Posta elettronica 8
6. Supporti esterni e dispositivi portatili 8
7. Siti di telelavoro 9
8. Regole per l'assistenza tecnica sugli strumenti elettronici e software 9
9. Piano di ripristino dei sistemi informatici e dei dati 9
9.1. Backup e DR 10
10. Log 11
11. Sistemi di protezione 11
11.1. Firewall 11
11.2. Rete wireless 12
12. Acquisizione di servizi e sistemi da soggetti esterni 12
13. Gestione delle anomalie, incidenti e punti di debolezza relativi alla sicurezza dei dati 12
13.1. Gestione delle anomalie 13
13.2. Gestione dell'incidente 14
14. Sanzioni 15
15. Entrata in vigore, riesame e aggiornamento 15

1. Oggetto e campo di applicazione del Regolamento

In conformità al Regolamento 679/2016/UE General Data Protection Regulation - GDPR, l'ASST Santi Paolo e Carlo intende attuare misure tecniche e organizzative adeguate, per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento dei dati comporta. Tale politica di sicurezza intende garantire:

1. la capacità di assicurare che sia convalidata l'integrità dei dati personali;
2. la capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
3. la capacità di ripristinare la disponibilità e l'accesso ai dati in modo tempestivo, in caso di incidente fisico o tecnico che abbia un impatto sulla disponibilità, sull'integrità e sulla riservatezza dei sistemi e dei servizi di informazione;
4. in caso di trattamento di dati personali sensibili, misure di sicurezza aggiuntive per garantire la consapevolezza dei rischi e la capacità di adottare in tempo reale azioni di prevenzione, correzione e attenuazione, contro le vulnerabilità riscontrate o gli incidenti verificatisi, che potrebbero costituire un rischio per i dati;
5. un processo per provare, verificare e valutare regolarmente l'efficacia delle politiche, delle procedure e dei piani di sicurezza attuati per assicurare la continua efficacia.

A tal fine l'ASST Santi Paolo e Carlo ha predisposto il presente Regolamento rivolto ai seguenti soggetti formalmente incaricati dalla Direzione ed **ai quali la Direzione ne richiede espressamente l'applicazione ed il rispetto**, per quanto di propria competenza:

- Responsabile Protezione dei Dati - RPD/ Data Protection Officer - DPO;
- Responsabile della sicurezza dei dati personali (interno);
- Amministratori di sistema;
- Responsabile IT;
- Incaricati all'assistenza e manutenzione degli strumenti elettronici;
- Incaricati alla custodia delle credenziali;
- Incaricati alla realizzazione e custodia delle copie di sicurezza delle banche dati.

Il *Responsabile della Protezione dei dati-RPD/Data Protection Officer-DPO* individuato dall'ASST Santi Paolo e Carlo è il seguente soggetto:

Cognome e nome	**E-mail**	**Telefono**
PERINATI PIERLUIGI MARIO	rpd@asst-santipaolocarlo.it	02.8184.2119

Il *Responsabile della sicurezza dei dati personali* individuato dall'ASST Santi Paolo e Carlo è il seguente soggetto:

Cognome e nome	**E-mail**	**Telefono**
SALA PIER MAURO	piermauro.sala@asst-santipaolocarlo.it	02.8184.2119

Gli *Amministratori di sistema* sono particolari soggetti individuati dall'ASST Santi Paolo e Carlo all'interno del personale delle società fornenti i servizi ICT e all'uopo autorizzati con apposita lettera.

Il *Responsabile IT* individuato dall'ASST Santi Paolo e Carlo è il seguente soggetto:

Cognome e nome	**E-mail**	**Telefono**
COCCHI ELLA	rpd@asst-santipaolocarlo.it	02.8184.3005

Gli *Incaricati all'assistenza e manutenzione degli strumenti elettronici* sono particolari soggetti individuati dall'ASST Santi Paolo e Carlo all'interno del personale delle società fornenti i servizi ICT e all'uopo autorizzati con apposita lettera.

Gli *Incaricati alla custodia delle credenziali* sono i seguenti soggetti:

Cognome e nome	**E-mail**	**Telefono**
COCCHI ELLA	rpd@asst-santipaolocarlo.it	02.8184.3005
ZIGONI STEFANIA	rpd@asst-santipaolocarlo.it	02.8184.3004

Gli *Incaricati alla realizzazione e custodia delle copie di sicurezza delle banche dati* sono particolari soggetti individuati dall'ASST Santi Paolo e Carlo all'interno del personale delle società fornenti i servizi ICT e all'uopo autorizzati con apposita lettera.

Il contenuto del presente Regolamento integra quanto disposto nel *Regolamento per la sicurezza del trattamento dei dati* approvato dalla Direzione.

L'oggetto del Regolamento sono le disposizioni stabilite dall'ASST Santi Paolo e Carlo per la gestione del sistema informativo atta a garantire la sicurezza del sistema stesso, assicurando la disponibilità delle risorse informative e dei dati, l'integrità dei sistemi e dei dati e la riservatezza delle informazioni.

2. Politiche generali

Le aree che contengono informazioni sensibili o critiche e strutture di elaborazione delle informazioni devono essere chiaramente definite e segnalate e ad accesso selezionato e controllato (si intende per accesso selezionato l'accesso consentito solo a personale specificatamente autorizzato, a titolo esemplificativo, tramite utilizzo di badge, chiavi ecc.).

Gli archivi che contengono informazioni sensibili o critiche devono essere ad accesso selezionato (si intende per accesso selezionato l'accesso consentito solo a personale specificatamente autorizzato, a titolo esemplificativo, tramite utilizzo di cassetti o armadi con serratura, cassaforte ecc.).

È necessario redigere e mantenere aggiornato l'inventario degli strumenti di gestione ed elaborazione delle informazioni.

I sistemi complementari quali sistemi di accesso, videosorveglianza, antintrusione, antincendio, climatizzazione ecc. messi a disposizione dall'ASST Santi Paolo e Carlo devono essere periodicamente revisionati e mantenuti in efficienza. In caso di rilevazione di malfunzionamento/anomalia di tali sistemi è necessario darne immediata comunicazione al responsabile individuato dall'ASST Santi Paolo e Carlo.

Le regole di sicurezza dei dati personali stabilite devono essere adeguate alla tipologia di dati trattati.

3. Accessi logici

La gestione degli accessi agli strumenti informatici aziendali deve rispettare i seguenti requisiti:

- i profili di autorizzazione per ciascun incaricato devono essere individuati e configurati anteriormente all'inizio del trattamento dei dati personali e, conseguentemente, preventivamente alla messa a disposizione degli strumenti informatici necessari per il trattamento;
- l'accesso deve avvenire tramite credenziali di autenticazione;
- gli accessi ed i permessi degli utenti devono essere mantenuti allineati ai profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento, seguendo le indicazioni del Titolare o del Responsabile dello specifico trattamento, se designato;
- le credenziali di autenticazione possono consistere in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo

oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato;

- il codice per l'identificazione (username), laddove utilizzato, in particolare quello per utenze di Amministratore di sistema, non deve essere assegnato ad altri incaricati, neppure in tempi diversi;
- se previste, le parole chiave (password) devono:
  - rispettare il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, minuscole, Maiuscole, simboli) e non devono essere riconducibili agevolmente all'incaricato;
  - essere modificate al primo utilizzo;
  - essere modificate almeno ogni sei mesi;
  - essere modificate almeno ogni tre mesi per i dati sensibili e giudiziari o altre informazioni critiche per l'ASST Santi Paolo e Carlo;
  - essere diverse da quelle precedenti;
- le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- le credenziali devono essere disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto;
- deve essere attivo un sistema di lockout in caso di errato inserimento credenziali oltre una soglia predefinita;
- per le sessioni di lavoro (Amministratore di sistema e non) devono essere impostati dei timeout di inattività;
- devono essere attivi gli screensaver protetti con password;
- in caso esistano servizi forniti attraverso reti pubbliche deve essere previsto un sistema di riconoscimento e di autenticazione sicuro;
- in caso di presenza di applicativi collegati a file database devono essere utilizzate credenziali di autenticazione sicure e regolarmente aggiornate per l'accesso a tali file.

Inoltre, per le utenze di Amministratore di sistema:

- devono essere utilizzate credenziali di elevata robustezza sostituite con sufficiente frequenza;
- deve essere assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli Amministratori, alle quali debbono corrispondere credenziali diverse;
- le utenze di Amministratore di sistema anonime, quali "Administrator", devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità a chi ne fa uso;
- è necessario redigere e mantenere aggiornato l'inventario di tutte le utenze di Amministratore di sistema, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata;
- l'utente amministrativo è tenuto a comunicare le proprie credenziali di autenticazione solo ed esclusivamente al soggetto incaricato alla custodia delle credenziali. Il documento deve essere sottoscritto dall'utente, sigillato in **busta chiusa** e consegnato *brevi manu* al soggetto su indicato. I dati comunicati verranno utilizzati esclusivamente dal soggetto Incaricato alla custodia delle credenziali nel caso di prolungata assenza o impedimento dell'utente. L'utilizzo delle credenziali riservate avverrà esclusivamente nell'ipotesi in cui si renda indispensabile intervenire per esclusive necessità di operatività e di sicurezza del sistema. L'incaricato alla custodia deve conservare le buste in luogo sicuro ad accesso controllato (locali chiusi a chiave, armadi e/o cassetti chiusi a chiave, cassaforte, etc.). Terminata l'assenza o l'impedimento dell'utente, lo stesso dovrà procedere alla modifica delle credenziali e a compilare nuovamente il modulo su indicato. Il soggetto Incaricato alla custodia delle credenziali informerà tempestivamente gli utenti, in qualità di incaricati al trattamento, nell'ipotesi di utilizzo delle loro credenziali di autenticazione.

Se è presente un dominio impostare tali regole a livello di dominio.

3.1. Procedura da adottare in caso di in caso di prolungata assenza o impedimento di un utente

In caso di prolungata assenza o impedimento di un utente che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, il responsabile IT, o altro soggetto formalmente incaricato, su indicazione della Direzione, al fine di assicurare la disponibilità dei dati e/o degli strumenti elettronici, per consentire l'accesso ad un altro utente indicato dalla Direzione, può:

- resettare in modo forzoso la componente riservata della credenziale di autenticazione;
- utilizzare la componente riservata della credenziale di autenticazione consegnata in busta chiusa.

Terminata l'assenza o l'impedimento dell'utente, lo stesso dovrà procedere alla modifica delle credenziali e, per i casi che prevedono l'utilizzo della busta chiusa, compilare nuovamente il documento su indicato.

Il soggetto Incaricato alla custodia delle credenziali informerà tempestivamente gli utenti nell'ipotesi di utilizzo delle loro credenziali di autenticazione.

4. Installazione, cambiamento e aggiornamento di apparecchiature informatiche

Le seguenti disposizioni regolano l'installazione di apparecchiature informatiche hardware e software (nuove o sostitutive) e, più in generale, il cambiamento o aggiornamento dell'infrastruttura tecnologica, al fine di eliminare o minimizzare il rischio di problematiche, incidenti o conflitti di competenza e di controllarne la rintracciabilità.

È fondamentale che per l'implementazione interna di un sistema o servizio e per i relativi aggiornamenti vengano rispettati:

- **il principio di privacy by design**, ossia la considerazione dei principi di riservatezza e protezione dei dati personali a partire dalla progettazione di un processo aziendale e delle relative applicazioni informatiche di supporto (in particolare la necessità di minimizzare l'uso del dato e la necessità di tutelare i diritti dell'interessato);
- **il principio di privacy by default**, ossia l'adozione di misure tecniche ed organizzative che garantiscano, per impostazione predefinita, che siano trattati solo i dati necessari per ogni specifica finalità del trattamento.

In particolare si richiede che per l'implementazione interna di un sistema o servizio e per i relativi aggiornamenti sia rispettata:

- la minimizzazione nella durata del trattamento dati;
- la minimizzazione nella tipologia di dati trattati;
- la minimizzazione nella quantità di dati trattati;
- la minimizzazione negli accessi ai dati;
- la limitazione del trattamento;
- la cancellazione dei dati;
- la possibilità di individuare una tempistica di conservazione dei dati;
- la garanzia di pseudonimizzazione dei dati;
- la garanzia di anonimizzazione dei dati;
- la garanzia di cifratura dei dati.

Prima di collegare alla rete un nuovo dispositivo è necessario che vengano sostituite le credenziali dell'Amministratore predefinito con valori coerenti con quelli delle utenze di Amministratore di sistema in uso.

Gli indirizzi IP assegnati agli strumenti devono essere registrati e aggiornati.

I dati presenti sugli strumenti informatici devono essere cancellati prima di procedere al loro riutilizzo, riassegnazione o smaltimento e deve essere tenuta evidenza della relativa cancellazione.

Le strutture di elaborazione delle informazioni devono essere posizionate in aree idonee chiaramente definite e segnalate e ad accesso selezionato e controllato.

L'installazione di apparecchiature informatiche hardware e software (nuove o sostitutive) deve rispettare tutte le disposizioni di sicurezza del presente Regolamento.

4.1. Messa in linea di server

Per la messa in linea di server è necessario seguire le seguenti indicazioni:

1. associare al server un identificativo univoco, che non potrà essere riutilizzato per nessun altro server (es. serial number o hostname);
2. registrazione dell'hardware all'interno della intranet aziendale;
3. test delle componenti hardware installate e configurazione degli strumenti di gestione (locale e remota) del server;
4. se il server non è nuovo (è stato utilizzato in precedenza per altri scopi), è necessario verificare che sia stato dismesso correttamente, e quindi sia in uno stato paragonabile a quello di "prima accensione";
5. installazione del sistema operativo (dettagliando codice univoco server, host name, descrizione server, stato, admin, IP, Vlan, SO, partizioni);
6. controlli post-installazione (connettività di rete nella Vlan impostata, anomalie log di sistema, funzionamento consolle amministrativa, funzionamento client o agenti di default, aggiornamento client o agenti);
7. posizionamento del server (considerare sicurezza fisica, occupazione spazio fisico, consumo elettrico, calore irradiato, connessione con altri apparati, accessibilità fisica, presenza di porte di connessione);
8. connessione dell'hardware con gli accessori e i cablaggi;
9. collegamento con NTP server per sincronizzazione degli orologi;
10. aggiornamento Topologia rete e Inventari.

4.2. Installazione e aggiornamento software e patch

È necessario redigere e mantenere aggiornato un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Le informazioni di inventario consentono un miglior controllo del processo di gestione dei software e delle patch. Potendo disporre di informazioni sugli aggiornamenti software installati o mancanti sui vari desktop è infatti possibile predisporre distribuzioni di software e relativi aggiornamenti, che garantiscono la conformità dell'ambiente desktop a una configurazione standard approvata a livello aziendale, in grado di assicurare livelli di prestazioni e di sicurezza prestabiliti.

Nel rispetto delle norme che regolano i diritti di proprietà intellettuale è obbligatorio utilizzare solo software originali e correttamente licenziati.

L'installazione, modifica e aggiornamento di software sugli strumenti deve essere permessa solo agli Amministratori.

È necessario, prima di procedere con l'installazione dei software e dei relativi aggiornamenti, eseguire un'attenta valutazione e analisi degli stessi.

È inoltre necessario rispettare le seguenti direttive:

1. verifica periodica dell'ambiente in cui applicare le patch, attraverso la definizione di livelli di sicurezza standard per i sistemi, il controllo costante dell'architettura di gestione delle patch e il controllo dell'efficienza;
2. identificazione delle installazioni e aggiornamenti software e valutazione della loro rilevanza nell'ambiente desktop;
3. analisi dei software e relativi aggiornamenti, per stabilire se il deployment richiede interventi particolari, valutando la necessità e le modalità di installazione;
4. eventuale definizione della sequenza con la quale verranno distribuiti nell'ambiente di produzione;
5. analisi dell'ambiente di produzione per verificare che gli strumenti dispongano di risorse sufficienti per la gestione dei nuovi software o aggiornamenti;
6. predisposizione di un piano di ripristino in caso di anomalie a seguito di installazione;
7. configurazione delle caratteristiche della distribuzione e dei pacchetti di installazione/aggiornamento, come la definizione dell'intervallo temporale consentito prima dell'installazione forzata e la gestione dei riavvii dei computer;
8. test di installazione/aggiornamento, ad esempio attraverso un'installazione pilota;
9. distribuzione dei software o aggiornamenti nell'ambiente di produzione;
10. verifica dell'esito della distribuzione.

Verificare che vengano installati gli aggiornamenti automatici del sistema operativo e dei vari programmi che tutelano la sicurezza degli strumenti elettronici (elaboratori e server).

Valutare l'aggiornamento a nuova versione o la sostituzione degli strumenti quando i produttori non rilasciano più aggiornamenti di sicurezza.

Deve essere utilizzato un sistema centralizzato di controllo automatico delle configurazioni che consenta di intercettare le modifiche non autorizzate.

Devono essere utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza, da utilizzare anche in occasione di ogni modifica significativa della configurazione.

5. Posta elettronica

I sistemi di posta elettronica, oltre a quanto previsto nel *Regolamento per la sicurezza del trattamento dei dati*, devono essere configurati in modo da non consentire l'apertura automatica dei messaggi di posta elettronica e non consentire l'anteprima automatica dei contenuti dei file.

6. Supporti esterni e dispositivi portatili

I dati devono essere cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento e deve essere tenuta evidenza della cancellazione.

In base al tipo di trattamenti eseguiti sui dispositivi portatili, deve essere valutata l'opportunità di dotarli di un sistema di cifratura dei dati contenuti nell'hard disk, affinché, qualora venga superato il meccanismo di autenticazione dell'accesso, comunque i dati risultino assolutamente indecifrabili.

I dispositivi portatili al fine di garantire il controllo, l'aggiornamento e l'allineamento alle politiche di sicurezza dell'ASST Santi Paolo e Carlo, devono essere periodicamente connessi, direttamente o tramite connessione protetta, alla rete aziendale, per la durata necessaria.

7. Siti di telelavoro

Al fine di proteggere le informazioni consultate, elaborate o memorizzate presso siti di telelavoro, è necessario che vengano rispettate tutte le disposizioni presenti nel *Regolamento per la sicurezza del trattamento dei dati* e nel presente documento.

I collegamenti con i siti di telelavoro devono inoltre essere gestiti tramite firewall, attraverso canali protetti e criptati.

Ove possibile e opportuno, bloccare il download in locale dei dati e/o attivare il log delle attività effettuate sui dati.

Oltre alle regole di autenticazione già elencate, implementare sistemi di riconoscimento sicuro degli utenti.

8. Regole per l'assistenza tecnica sugli strumenti elettronici e software

La manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo devono essere pianificati e svolti periodicamente e ne deve essere tenuta registrazione.

Si elencano le operazioni da eseguire per garantire la sicurezza, la protezione e riservatezza dei dati personali nell'ipotesi in cui si verifichi la necessità di effettuare interventi di assistenza tecnica (manutenzione ordinaria o straordinaria e aggiornamento) sugli strumenti elettronici e software, da parte del personale interno all'ASST Santi Paolo e Carlo (Incaricato all'assistenza e manutenzione degli strumenti elettronici) e/o da parte di soggetti esterni (outsourcing):

- predisporre credenziali di autenticazione dedicate che permettano l'accesso amministrativo specifico, da parte del personale tecnico, allo strumento elettronico (server e/o elaboratore) su cui è necessario effettuare l'intervento;
- analogamente nell'ipotesi di interventi di assistenza tecnica effettuata da remoto da parte di soggetti terzi, l'accesso ai sistemi informatici deve essere consentito esclusivamente tramite una credenziale di autenticazione dedicata (username e password) fornita dal soggetto Incaricato all'assistenza e manutenzione degli strumenti elettronici dell'ASST Santi Paolo e Carlo. La credenziale deve essere disattivata al termine dell'intervento (l'utilizzo di un sistema operativo "sicuro" garantisce che ad un successivo intervento non sarà possibile accedere con la medesima credenziale di autenticazione);
- nell'ipotesi in cui gli interventi tecnici vengano effettuati da personale esterno all'ASST Santi Paolo e Carlo (outsourcing), questo deve fornire una dichiarazione scritta attestante la conformità dell'intervento alla normativa in materia di privacy;
- nell'ipotesi di assistenza e/o adeguamento tecnico effettuato da remoto da parte di aziende esterne, indicare il nominativo del soggetto che esegue l'assistenza e garantire che il collegamento venga autorizzato solo dall'IP chiamante (tramite collegamento cifrato e criptato). Al termine delle operazioni di adeguamento, deve essere rilasciato un modulo di intervento che attesti la conformità delle operazioni eseguite alle disposizioni normative in ambito di protezione dei dati personali.

L'esecuzione di tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature deve avvenire per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

9. Piano di ripristino dei sistemi informatici e dei dati

Le procedure di ripristino dei sistemi informatici e dei dati devono essere raccolte nei documenti che individuano l'insieme delle misure tecnologiche e organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie, affinché l'attività dell'ASST Santi Paolo e Carlo non venga interrotta a fronte di gravi emergenze.

Le procedure di ripristino dei sistemi informatici e dei dati permettono all' ASST Santi Paolo e Carlo di far fronte ad eventi imprevisti, che minacciano l'infrastruttura informatica. Le componenti informatiche che con maggiore frequenza possono essere colpite da eventi imprevisti sono i dispositivi hardware, software, reti, processi produttivi e di gestione. Proteggere gli investimenti dell'infrastruttura tecnologica dell'ASST Santi Paolo e Carlo e la sua capacità di svolgere la propria attività sono i motivi principali per attuare le procedure di ripristino dei sistemi informatici.

Premesso ciò, deve essere predisposto un sistema che garantisca il recupero dei dati e la disponibilità degli strumenti elettronici con idonee procedure di backup e di ripristino come disposto dalla normativa in materia privacy.

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

9.1. Backup e DR

È necessario ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, oltre che l'accesso non autorizzato o il trattamento non consentito o non conforme alle finalità della raccolta, i rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto di trattamento.

A tal fine è indispensabile adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.

Deve quindi essere previsto un sistema di salvataggio con le seguenti caratteristiche minime:

- backup dei dati / sistemi, individuale o centralizzato, con una periodicità adeguata;
- sistema di log del sistema di backup;
- sistema di disaster recovery esterno;
- sistema di verifica della corretta esecuzione dei backup/DR;
- backup protetti e custoditi in luoghi sicuri ad accesso selezionato e controllato.

La pianificazione del processo deve prevedere un orario di replica tale da non influire sul singolo trattamento delle banche dati da parte degli Incaricati (a tal fine i salvataggi dovrebbero essere effettuati al termine del normale orario di lavoro) e deve assicurare una selezione scrupolosa delle informazioni (sistemi e/o dati) che devono essere oggetto di backup.

Ricordarsi che devono essere oggetto di backup anche i dati presenti sui dispositivi portatili (notebook, tablet, smartphone ecc.), qualora su tali dispositivi risiedano dati che non prevedono un processo di salvataggio centralizzato.

La pianificazione del processo di salvataggio deve essere aggiornata ad ogni variazione della posizione di dati e sistemi.

Deve essere effettuato un test di ripristino periodico sui sistemi di backup/DR.

I supporti contenenti almeno una delle copie di backup non devono essere permanentemente accessibili dal sistema, onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

I dispositivi utilizzati per effettuare le copie di sicurezza dei dati informatici devono inoltre essere resi possibilmente intelligibili e custoditi in luogo sicuro ad accesso controllato e selezionato.

Ove possibile devono essere centralizzati i dati su un unico dispositivo (Server, NAS, PC che funge da Server) al fine di prevedere un unico salvataggio di tutti i dati personali trattati.

È necessario applicare la ridondanza agli asset informatici strategici e critici, quali, a titolo indicativo, server e backup.

Le immagini d'installazione devono essere memorizzate offline.

Deve essere tenuta evidenza delle attività inerenti le operazioni di backup, ripristino e test di ripristino.

L'ASST Santi Paolo e Carlo può individuare, tramite lettera di nomina, il soggetto Incaricato alla realizzazione e alla custodia delle copie di sicurezza dei dati personali.

10. Log

Deve essere attivato un sistema di log degli Amministratori, con dati di log immodificabili e che preveda un riesame periodico da parte di soggetto diverso dagli Amministratori stessi.

Deve essere attivato un sistema di log degli eventi, con dati di log immodificabili.

Gli strumenti per la raccolta dei log e le informazioni di log devono essere protette da manomissioni e accessi non autorizzati.

11. Sistemi di protezione

Devono essere presenti e aggiornati idonei sistemi di protezione da malware, impostati in modo da scaricare automaticamente gli aggiornamenti.

Devono essere presenti e aggiornati idonei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti (antivirus, antispy, antispam, etc.).

Devono essere periodicamente eseguite le scansioni con i sistemi di protezione, anche per rilevare eventuali vulnerabilità.

Ove possibile, deve essere configurato un sistema di controllo di attività anomale sulla rete e sui sistemi (idonea protezione contro Distributed Denial of Services attack e sistema di lockout a livello di IP per le richieste anomale).

I punti rete non utilizzati devono essere disabilitati.

La rete dati deve essere certificata.

È necessario che vengano eseguite regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato e/o di modifiche alle configurazioni standard impostate dall'area IT.

Per i dati sensibili e giudiziari o comunque per le informazioni critiche è necessario implementare un sistema di protezione tramite crittografia o password, soprattutto in caso di trasmissione degli stessi.

Dotare i server e gli elaboratori di un gruppo di continuità, al fine di prevenire la perdita accidentale dei dati dovuta a sbalzi di tensione, spurie sulla rete o mancanza di alimentazione.

11.1. Firewall

Deve essere presente un firewall (hardware e/o software) per tutti i dispositivi collegati in rete (individuale o centralizzato), assicurandosi che tutte le porte siano chiuse ed annotando, inoltre, eventuali porte che devono essere lasciate aperte per necessità operative.

Deve essere attivo un sistema di lockout sulle porte dei firewall in caso di errati tentativi di accesso multipli.

Per gli accessi dall'esterno (a titolo esemplificativo collegamento tra sedi) prevedere, ove possibile, regole che garantiscano collegamenti a indirizzi IP sicuri e selezionati.

Le porte non utilizzate devono essere disabilitate.

Se la rete è aperta all'esterno deve essere su una DMZ appositamente definita.

Per gli strumenti che hanno accesso a Internet deve essere attivo un sistema di controllo e limitazione della navigazione Internet.

L'accesso dall'esterno deve essere protetto da credenziali di autenticazione e consentito solo a personale autorizzato.

Devono essere registrati gli accessi ed i tentativi di accesso dall'esterno alla rete.

11.2. Rete wireless

La rete wireless deve essere protetta e criptata.

Se la rete wireless non è aperta ai soli utenti profilati ed autorizzati dall'ASST Santi Paolo e Carlo, la rete wireless aperta deve essere separata da quella interna.

La rete wireless esterna deve avere filtri e controlli alla navigazione.

Devono essere attivate idonee procedure di sicurezza per i sistemi wireless (mac address e criptatura dei dati).

12. Acquisizione di servizi e sistemi da soggetti esterni

L'ASST Santi Paolo e Carlo deve essere in possesso e conservare le condizioni contrattuali applicate dai fornitori di servizi inerenti il trattamento di dati relativamente ai meccanismi di sicurezza, ai livelli di servizio ed ai requisiti di gestione.

Deve essere eseguito il monitoraggio, riesame e audit sui servizi erogati dai fornitori che hanno impatto sulla sicurezza dei dati, anche in occasione di variazioni.

Deve essere richiesta la compliance privacy by design, ossia la considerazione dei principi di riservatezza e protezione dei dati personali a partire dalla progettazione di un processo aziendale e delle relative applicazioni informatiche di supporto, e by default, ossia privacy come principio di base, per l'acquisto e/o per lo sviluppo in outsourcing di sistemi informativi o di servizi affidati all'esterno e per i relativi aggiornamenti, compresi i rilasci di nuove versioni.

13. Gestione delle anomalie, incidenti e punti di debolezza relativi alla sicurezza dei dati

La gestione delle anomalie e punti di debolezza e la gestione degli incidenti ha l'obiettivo di risolvere il più velocemente ed efficacemente possibile un evento che impattata, più o meno

gravemente, sulla sicurezza, riservatezza, disponibilità e integrità dei dati e sul regolare funzionamento del sistema informatico.

Si intende "anomalia" o "punto di debolezza" un qualsiasi evento non previsto che:

- ha impatto limitato su servizi non critici e che non causa blocco di operatività del sistema o perdita o degrado di informazioni;
- si riferisce all'operatività di un singolo utente o di un gruppo molto esiguo di utenti;
- è risolto in maniera automatica dai controlli tecnologici messi in campo e non richiede altri interventi manuali per il suo ripristino.

Sono esempi di anomalie: segnalazioni di aggressioni da virus informatico rimosse automaticamente dal software antivirus; interruzioni temporanee di alimentazione coperte dall'UPS; guasti singoli ai PC degli utenti o qualsiasi segnalazione di malfunzionamento limitata al singolo utente; tracce di attacco rilevate dal firewall o dai proxy ma senza impatto sui servizi; comportamenti anomali di una stazione, di un utente o di un servizio ma senza impatti sull'infrastruttura.

Le anomalie sono considerate eventi comuni e inevitabili nella normale operatività del sistema. Sono gestite direttamente dal personale IT.

Si intende "incidente" un qualsiasi evento non previsto che:

- incide sulla funzionalità completa di uno o più servizi;
- comporta superamento delle barriere di sicurezza perimetrale o di protezione da virus informatici, con conseguente grave rischio di compromissione dei requisiti di sicurezza delle informazioni;
- richiede l'intervento delle forze dell'ordine;
- causa la permanenza dell'infrastruttura per periodi prolungati in condizioni di potenziale rischio.

Sono esempi di incidente: l'anomalia che riguardi aspetti relativi alla privacy degli interessati oppure che possa rientrare nella sfera delle responsabilità di tipo legale; la rilevazione di un accesso non autorizzato a locali tecnologici; l'attacco diffuso da virus informatici non rimosso dal sistema antivirus; il blocco prolungato di parte di un sistema ridondato, tale per cui ne resti in linea solo una delle due repliche; intrusioni nella rete interna o compromissione dei servizi informatici; anomalie ripetute sistematicamente o che coinvolgono un ampio numero di utenti o che impattano potenzialmente su dati sensibili, giudiziari o comunque critici per l'ASST Santi Paolo e Carlo.

Gli incidenti sono eventi eccezionali, che prevedono obbligatoriamente il coinvolgimento del Responsabile IT e della Direzione.

Quando l'incidente rilevato dovesse comportare la completa indisponibilità operativa o la perdita definitiva di componenti del sistema informatico per disastro ambientale o cause di forza maggiore, l'incidente è classificato come disastro e trattato secondo il "Piano di Continuità Operativa " se presente.

13.1. Gestione delle anomalie

L'anomalia o punto di debolezza può essere rilevata automaticamente dal sistema o segnalata dagli utenti. Qualora il personale IT la qualifichi come incidente deve darne immediata comunicazione al responsabile IT.

L'anomalia è risolta automaticamente o manualmente dal personale IT.

Qualora il personale IT, dall'analisi delle anomalie, ravvisi un potenziale punto di debolezza nel sistema, ad esempio in caso di recidive, deve darne comunicazione al responsabile IT, che

procederà con la relativa valutazione, eventualmente sentendo il Responsabile della sicurezza dei dati e/o la Direzione, e con l'eventuale necessario intervento tecnico.

L'anomalia deve essere archiviata nel sistema di log automatico dello strumento tecnico impiegato per la sua gestione oppure mantenendone evidenza tramite ulteriori strumenti a disposizione. È vietato cancellare o modificare tali registrazioni.

13.2. Gestione dell'incidente

Le modalità con cui un incidente viene rilevato consistono in una comunicazione al Responsabile IT da parte dell'utente che lo ha rilevato e/o mediante strumenti di monitoraggio e gestione eventi.

Il responsabile IT deve darne immediata comunicazione alla Direzione che provvederà a incaricare un Responsabile per la gestione dell'incidente.

Quest'ultimo deve identificare le cause, definire l'intervento per la risoluzione tempestiva dell'incidente, predisporre un piano di intervento che preveda attività da porre in essere, incaricati, tempistiche e risorse. Devono inoltre essere individuati gli eventuali fattori che potrebbero causare il ripetersi dell'incidente.

Qualora il responsabile IT ravvisi l'impossibilità di risolvere l'incidente in un tempo accettabile è necessario identificare rimedi temporanei per procedere in prima istanza al ripristino del servizio. In secondo luogo è possibile procedere all'implementazione delle misure risolutive dell'incidente.

L'incidente può essere considerato risolto solo trascorso un tempo ragionevole dal ripristino del servizio per la verifica dell'efficacia dell'intervento (non ripetersi dell'incidente, analisi eventuali ripercussioni non previste, verifica mantenimento parametri di normalità).

Il Responsabile IT è tenuto a tenere costantemente aggiornata la Direzione sullo stato di avanzamento del Piano di intervento ed a registrare un Rapporto di incidente (tramite apposito modulo o tramite procedura software). Il Rapporto di incidente deve avere i seguenti contenuti minimi:

- descrizione incidente;
- modalità di rilevamento;
- responsabile di gestione dell'incidente;
- analisi delle cause;
- piano di gestione;
- attività e incaricati delle attività da porre in essere;
- tempistiche previste ed effettive;
- risorse messe a disposizione;
- attività effettivamente eseguite;
- test eseguiti;
- verifica efficacia intervento.

Al termine del processo di gestione dell'incidente può procedere alla chiusura dello stesso, previa autorizzazione della Direzione.

La registrazione dell'incidente e delle operazioni di gestione è fondamentale per l'ASST Santi Paolo e Carlo al fine di creare una base di conoscenza per evitare il ripetersi dello stesso e per aumentare la sicurezza del sistema informativo aziendale.

In caso si verifichi una violazione dei dati personali (Data Breach), ossia una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati è necessario darne immediata comunicazione al Responsabile del Trattamento o al

Responsabile della Protezione dei Dati - RPD o al Titolare, affinché possano attivare le procedure di notifica previste dalla legge così come stabilite e dettagliate dalla *Procedura di Gestione del Data Breach*.

14. Sanzioni

È fatto obbligo ai soggetti di cui all'articolo 1 del presente documento osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente C.C.N.L. applicabile, nonché con tutte le azioni civili e penali consentite anche nei confronti di collaboratori e professionisti.

15. Entrata in vigore, riesame e aggiornamento

Il presente regolamento è in vigore a partire dal 20/12/2018.

Il Regolamento viene riesaminato ed aggiornato con cadenza periodica annuale o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

PROCEDURA DI GESTIONE DEL DATA BREACH

1. Introduzione

La presente procedura ha lo scopo di gestire il necessario flusso di attività da porre in essere nel momento in cui si sviluppi una violazione di dati personali ai sensi degli articoli 33 e 34 del Regolamento 679/2016/UE.

La procedura verrà avviata attraverso la compilazione di un questionario on-line presente all'interno del sistema MUA – Motore Unico Amministrativo – e coinvolgerà le diverse unità organizzative che segnaleranno l'avvenuta violazione, la funzione interna competente in materia di protezione dei dati ed il Data Protection Officer (DPO).

2. Casi nei quali avviare la procedura Data Breach

I casi nei quali avviare una procedura Data Breach saranno i seguenti:

2.1 Sottrazione di credenziali di autenticazione;

2.2 Furto di PC, Notebook, Tablet, Smartphone contenente dati personali;

2.3 Erronea diffusione, pubblicazione, comunicazione di dati personali;

2.4 Intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali;

2.5 Furto di archivi cartacei e/o digitali;

2.6 Accesso non autorizzato nel sistema informativo aziendale;

2.7 Azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza aziendali;

2.8 Smarrimento di dati personali (archiviati su supporti cartacei e digitali);

2.9 Distruzione di dati personali (archiviati su supporti cartacei e digitali).

3. Soggetti obbligati ad avviare la procedura di gestione della violazione

- Titolare del trattamento;
- Responsabili del trattamento;
- Gruppo Privacy;
- DPO;

4. Modalità di avvio della procedura di gestione della violazione

L'avvio della procedura di gestione Data Breach dovrà essere sviluppata seguendo le seguenti fasi:

4.1 accedere al sistema MUA attraverso l'indirizzo web https://mua.secoges.com;

4.2 inserire le proprie credenziali di autenticazione;

4.3 cliccare il pulsante all'interno della home page denominato "Workflow per ambito normativo";

4.4 cliccare sul simbolo "+" accanto alla dicitura "Pacchetto privacy"

4.5 cliccare sulla dicitura "Privacy – Data Breach"

4.6 rispondere alle domande del questionario.

Il questionario si articola in successivi passaggi denominati STEP ognuno dei quali riguarda differenti tipi di informazioni legate al Data Breach o alla sua comunicazione al Garante e/o agli interessati. Tali informazioni sono descritte dettagliatamente, a passo a passo, nel flusso rappresentato al successivo punto 6..

Si tenga presente che siccome MUA è stato popolato con la descrizione dell'infrastruttura fisica e tecnologica dell'ente allora il sistema chiederà di selezionare i luoghi fisici e/o le componenti informatiche oggetto della violazione da un elenco a tendina che il sistema medesimo suggerirà; qualora invece, nonostante l'avvenuto popolamento, l'oggetto della violazione non sia presente all'interno del software verrà chiesto di compilare dei campi testo all'interno dei quali descrivere la violazione verificatasi (vedasi lo STEP A del flusso rappresentato al successivo punto 6.).

Ogni Step si conclude con un salvataggio dei dati e delle informazioni inserite. Gli Step sono:

Step A. Prima identificazione violazione incidente;

Step B. Controlli necessità della notifica al Garante;

Step C. Compilazione del modulo di comunicazione;

Step D. Controlli necessità della comunicazione agli interessati;

Step E. Chiusura dell'incidente.

Solo gli Step A, B ed E sono sempre effettuati, gli altri step dipendono dalla valutazione di gravità che viene fatta in prima battuta dal sistema e quindi dal DPO, dal Gruppo Privacy ed infine , quale ultima parola, dal legale rappresentante del Titolare del trattamento; solo a seguito di accertata gravità saranno eseguiti gli step C e D. La chiusura dell'incidente avverrà con la dichiarazione di avvenuta segnalazione al Garante e/o agli interessati ovvero con la dichiarazione che il Data Breach non è grave. Responsabile dell'invio di dette segnalazioni ovvero della registrazione in MUA della dichiarazione di gravità è il DPO. Responsabile della stesura del verbale dell'avvenuto Data Breach è il Gruppo Privacy che lo sottopone per la firma al legale rappresentante del Titolare del trattamento. Quest'ultimo può adottare differenti comportamenti rispetto a quanto proposto e ne indica le motivazioni nel verbale stesso.

5. Valutazioni del DPO ed eventuali comunicazioni (artt. 33 e 34 Regolamento 679/2016/UE)

Una volta conclusa la fase di avvio della procedura, il sistema "ingaggerà" il DPO al fine di verificare la necessità di convocare il Gruppo Privacy per effettuare le opportune valutazioni sulla eventuale necessità di sviluppare una comunicazione dell'evento all'Autorità Garante e sulla eventuale necessità di sviluppare una comunicazione agli interessati.

Qualora siano necessarie le comunicazioni di cui agli artt. 33 e/o 34 del Regolamento 679/2016/UE, il DPO provvederà a contattare il gruppo Privacy che nel suo insieme, sulla scorta della segnalazione ricevuta, sulle indicazioni fornite dal DPO e su ulteriori informazioni fornite dal Responsabile (interno od esterno)del trattamento e da eventuali incaricati che hanno segnalato il si occuperà di realizzare il contenuto del verbale dell'occorso Data Breach e di sottoporlo al legale rappresentante del Titolare del Trattamento per la sottoscrizione.

Qualora non siano necessarie comunicazioni il DPO provvederà alla chiusa dell'evento di violazione la cui traccia rimarrà all'interno di apposito registro contenuto nel sistema MUA e reperibile all'interno del sistema stesso, nella pagina "Elementi di analisi", alla voce "Regolamento 679/2016/UE - Data Breach".

Qualora viceversa siano necessarie comunicazioni il DPO provvederà all'invio del Modulo di comunicazione al Garante e/o alla notifica agli interessati dell'evento di violazione occorso.

Si rappresenta di seguito un flusso schematico delle informazioni oggetto della procedura di gestione Data Breach.

6. Flusso schematico delle informazioni

Step A. Prima identificazione violazione incidente

Selezione gli strumenti hardware o software/i locali fisici/gli strumenti oggetto della violazione/Incidente

↓

Data e l'ora della violazione/incidente

↓

Nominativo del soggetto che ha rilevato la violazione/incidente

↓

Modalità di rilevazione della violazione/incidente

↓

Possibili cause della violazione/incidente

↓

Tempi necessari per la risoluzione della problematica

↓

Periodo della violazione è stato determinato

↓

Indicazione se la violazione è avvenuta all'interno o all'esterno dell'Ente titolare

- SE INTERNO: l'utente deve selezionare il locale (o più di un locale) tra quelli mappati nel sistema
- SE ESTERNO: il sistema richiede l'indirizzo della sede in cui è avvenuta la violazione e la specifica di ulteriori informazioni utili che dettaglino con maggiore precisione il luogo in questione

↓

Indicazione se la violazione/incidente è avvenuta a seguito di smarrimento di supporti portatili o dispositivi mobili

↓

Tipo di violazione

↓

Misure applicate ai dati oggetto della violazione

↓

Incarico al DPO per proseguire con le fasi successive del flusso

Step B. Controlli necessità della notifica al Garante

Controllo da parte del sistema che tra le categorie di dati dei trattamenti (legati agli strumenti selezionati come oggetto della violazione/incidente) ci siano dati biometrici oppure che riguardi il dossier sanitario

↓

Verifica che la violazione/incidente presenti rischi per i diritti e le libertà delle persone fisiche

•SI: in base alle categorie di dati rilevati, il sistema definisce i tempi entro i quali è necessario effettuare la comunicazione all'autorità di controllo (24/48/72 ore) (si prosegue con il successivo Step C)

•NO: il sistema dichiara che è necessaria la mappatura delle caratteristiche della violazione/incidente ma non la comunicazione dell'avvenuta violazione all'autorità di controllo (si passa allo Step E)

Step C. Compilazione del modulo di comunicazione

Indicazione dell'indirizzo mail/pec su cui ricevere eventuali comunicazioni

↓

Recapito telefonico

↓

Persone colpite dalla violazione

- Numero conosciuto: indicare il numero preciso o indicativo delle persone colpite dalla violazione/incidente

OPPURE

- Numero sconosciuto: il sistema memorizza l'informazione

↓

Indicazione del livello di gravità della violazione

↓

Indicazione se la violazione coinvolge interessati che si trovano in altri Paesi UE

- SI: indicazione dell'eventuale autorità a cui è stata inviata la comunicazione

Step D. Controlli necessità della comunicazione agli interessati

Verifica se la violazione/incidente può comportare o essere connessa ai rischi per l'interessato ai fini della valutazione della necessità di:

- di effettuare la comunicazione all'interessato
- di non effettuare la comunicazione all'interessato
- di non effettuare la comunicazione all'interessato ma di effettuare una comunicazione pubblica

Step E. Chiusura dell'incidente

Produzione del documento circa la comunicazione dell'avvenuta violazione da inviare all'autorità di controllo (quando necessaria), attraverso la firma della persona responsabile (soggetto addetto alle comunicazioni al Garante).