REGOLAMENTO PER LA GESTIONE DEL SISTEMA INFORMATIVO

Sistema Socio Sanitario
Regione Lombardia
ASST Santi Paolo e Carlo

Sommario

Sistema Socio Sanitario
Regione Lombardia
ASST Santi Paolo e Carlo

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.