COMUNE DI SANT'ANGELO DI BROLO

C.A.P. 98060 CITTA' METROPOLITANA DI MESSINA C.F. 00108980830

Ufficio del Responsabile per la Transizione Digitale

REGOLAMENTO PER LA GESTIONE DEL SISTEMA INFORMATIVO

Sommario

Introduzione

Il presente regolamento traccia le linee per la gestione e la sicurezza del sistema informativo del Comune di Sant'Angelo di Brolo garantendo, nel contempo, la disponibilità delle risorse informative e dei dati, l'integrità dei sistemi informatici e la riservatezza delle informazioni.

1. Oggetto e campo di applicazione

In conformità al Regolamento 679/2016/UE General Data Protection Regulation - GDPR, si rende necessario individuare ed applicare misure tecniche ed organizzative adeguate garantire un livello di sicurezza appropriato in relazione ai rischi che il trattamento dei dati comporta.

La politica di sicurezza tracciata dal presente documento intende promuovere e garantire:

1. l'applicazione di misure atte ad assicurare l'integrità dei dati personali;
2. la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
3. l'adozione di misure idonee a ripristinare la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico che abbia un impatto sul funzionamento, sull'integrità e sulla riservatezza dei sistemi e dei servizi di informazione;
4. l'adozione, in tempo reale, di azioni di prevenzione, correzione ed attenuazione delle vulnerabilità riscontrate o degli incidenti che potrebbero comportare un pericolo per il trattamento di dati personali sensibili attraverso misure di sicurezza aggiuntive per il contrasto dei rischi;
5. l'adozione di processi di prova, verifica e valutazione dell'efficacia delle politiche, delle procedure e dei piani di sicurezza previsti.

A tal fine l'Ente ha predisposto il presente Regolamento rivolto ai seguenti soggetti formalmente incaricati per quanto di rispettiva competenza:

- Data Protection Officer - DPO;
- Responsabile della sicurezza dei dati personali interno;
- Amministratore/i di sistema;
- Responsabile IT;
- Incaricati all'assistenza e manutenzione degli strumenti elettronici;
- Incaricati della custodia delle credenziali;
- Incaricati della realizzazione e della custodia delle copie di sicurezza delle banche dati.

Il contenuto del presente atto integra quanto disposto nel Regolamento per l'implementazione di misure organizzative e processi interni sulla protezione dei dati personali in attuazione del Regolamento (UE) 679/2016 approvato dall'Ente con Delibera di Consiglio Comunale n. 36 del 05/07/2019.

Costituiscono oggetto del presente regolamento le disposizioni minime individuate dell'Ente per la gestione del sistema informativo idonea 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. Criteri 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 prevedere modalità di accesso selezionato (si intende tale l'accesso consentito solo a personale a ciò specificatamente autorizzato).

A tal fine occorre 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. 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'Ente.

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 preliminarmente all'inizio del trattamento dei dati personali e 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 coerenti con i profili di autorizzazione degli incaricati del trattamento dei dati, in modo da limitare l'accesso esclusivamente ai dati occorrenti ad eseguire le operazioni di trattamento secondo le indicazioni del Titolare del Trattamento o del Responsabile dello specifico trattamento, ove designato;
- le credenziali di autenticazione possono consistere in un codice per l'identificazione dell'incaricato associato a una parola chiave personale 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, è personale e 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'Ente;
  - essere diverse da quelle precedenti;
- le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate salvo quelle preventivamente autorizzate per attività di gestione tecnica;
- le credenziali devono essere disattivate anche in caso di trasferimento ad altro servizio, di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico ed ai dati personali in esso custoditi o all'area ad accesso riservato;
- deve essere attivo un sistema di l*ockout* in caso di errato inserimento credenziali oltre una soglia predefinita;
- per le sessioni di lavoro (amministrative e non) devono essere impostati dei *timeout* di inattività;
- devono essere attivi gli screensaver protetti con password;
- per i servizi forniti attraverso reti pubbliche deve essere previsto un sistema di riconoscimento e di autenticazione sicuro;
- per eventuali applicativi collegati a file database devono essere utilizzate credenziali di accesso ed autenticazione sicure e regolarmente aggiornate.

Inoltre, per le utenze amministrative:

- devono essere utilizzate credenziali di elevata robustezza da cambiare con adeguata frequenza;
- deve essere assicurata la netta distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse;
- le utenze amministrative 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 esclusivamente a chi ne fa uso;

- è necessario redigere e mantenere aggiornato l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia formalmente autorizzata;
- ogni utente amministrativo è tenuto a comunicare le proprie credenziali di autenticazione al soggetto incaricato alla custodia delle credenziali in **busta chiusa e sigillata** consegnata *brevi manu*; le credenziali potranno essere utilizzate esclusivamente dal soggetto Incaricato della loro custodia nel caso di prolungata assenza od impedimento dell'utente; l'utilizzo delle credenziali riservate potrà avvenire soltanto qualora si renda indispensabile intervenire per esclusive necessità operative 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 documento indicato; il soggetto Incaricato della custodia delle credenziali informerà tempestivamente gli utenti in caso di utilizzo delle loro credenziali di autenticazione.

Se è presente un dominio tali regole saranno applicate a livello di dominio.

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

In caso di prolungata assenza od 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 dall'Ente, 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 la componente riservata della credenziale di autenticazione;
- utilizzare la componente riservata della credenziale di autenticazione consegnata in busta chiusa.

Al cessare dell'assenza o dell'impedimento dell'utente, questi 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 sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative 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 rete 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 che si trovi 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 (sicurezza fisica, spazio fisico, consumo elettrico, calore irradiato, connessione con altri apparati, accessibilità fisica, porte di connessione);
8. connessione dell'hardware con gli accessori e i cablaggi;
9. collegamento con NTP server per la 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 sistema 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 conseguenti ad interventi di installazione/aggiornamento;
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;
9. verifica dell'esito.

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.

Utilizzare strumenti di scansione delle vulnerabilità della sicurezza, regolarmente aggiornati da impiegare 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 né 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 rimovibili prima di procedere al loro riutilizzo, riassegnazione o smaltimento e l'avvenuta cancellazione dev'essere riscontrabile da apposita annotazione di servizio .

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, i dati risultino assolutamente indecifrabili.

I dispositivi portatili al fine di garantire il controllo, l'aggiornamento e l'allineamento alle politiche di sicurezza adottate dall'Ente, 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, bloccando, ove possibile, il download in locale dei dati e/o attivare il log delle attività effettuate sui dati ed implementando i 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.

Per garantire la sicurezza, la protezione e riservatezza dei dati personali qualora si debbano effettuare interventi di assistenza tecnica (manutenzione ordinaria o straordinaria e aggiornamento) sugli strumenti

elettronici e software, da parte del personale interno all'Organizzazione (Incaricato all'assistenza e manutenzione degli strumenti elettronici) e/o da parte di soggetti esterni (outsourcing) occorre che :

- vengano predisposte 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;
- 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'Organizzazione. 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); qualora gli interventi tecnici vengano effettuati da personale esterno all'Organizzazione (outsourcing), questo deve fornire una dichiarazione scritta attestante la conformità dell'intervento alla normativa in materia di privacy; in caso 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 riattivazione dei sistemi informatici e dei dati devono essere previste nei documenti che individuano l'insieme delle misure tecnologiche ed organizzative atte al ripristino di sistemi, dati e infrastrutture necessari a garantire la continuità funzionale delle attività istituzionali anche a fronte di gravi emergenze.

Sono da considerare a rischio i dispositivi hardware, software, le reti, i processi produttivi e di gestione.

Per ridurre e contrastare i rischi occorre predisporre 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, in base alla tecnologia disponibile, alla tipologia dei dati e alle specificità di ogni procedimento, riducendo al minimo, attraverso 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, con modalità e tempistiche compatibili con i diritti degli interessati.

Occorre prevedere 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) oggetto di backup.

Devono costituire oggetto di backup anche i dispositivi portatili (notebook, tablet, smartphone ecc.), qualora su di essi 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.

Per garantire la conservazione dei dati e la possibilità di ripristino occorre che una delle copia di backup non sia permanentemente accessibile dal sistema.

I dispositivi utilizzati per eseguire le copie di sicurezza dei dati informatici debbono custodirsi in luogo sicuro ad accesso controllato e selezionato.

Occorre prevedere, ove possibile, la custodia centralizzata dei dati su un unico dispositivo (Server, NAS, PC che funge da Server) adottando un sistema di salvataggio univoco.

È necessario applicare i principio di ridondanza dei dati agli asset informatici strategici ed a maggior rischio quali server e backup.

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

L'Ente può individuare, tramite lettera di nomina, uno o più soggetti incaricati della realizzazione e della custodia delle copie di sicurezza dei dati.

10. Log

Deve essere attivato un sistema di log degli amministratori, con dati di log immodificabili 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 in via cautelare 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 è opportuno prevedere una DMZ .

Per gli strumenti che hanno accesso ad 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'Ente, la rete wireless aperta deve essere separata da quella interna.

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

Possono essere attivate procedure di sicurezza per i sistemi wireless (mac address o criptatura dei dati).

12.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 tempestivamente ed efficacemente ogni evento che possa ripercuotersi 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 un impatto limitato su servizi non critici e non causa il blocco di operatività del sistema né perdita od il degrado di informazioni;
- si riferisce all'operatività di un singolo utente o di un gruppo ristretto di utenti;
- si risolve in modo automatico attraverso le tecnologie di controllo attive e non richiede 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 ed 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 il superamento delle barriere di sicurezza perimetrale o di protezione da virus informatici con conseguente rischio di compromissione dei requisiti di sicurezza delle informazioni;
- richiede l'intervento delle forze dell'ordine;
- determina il permanenza dell'infrastruttura in condizioni di potenziale rischio per periodi prolungati.

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 che lasci efficiente soltanto una delle due repliche; le intrusioni nella rete interna o la compromissione dei servizi informatici; le anomalie ripetute sistematicamente o tali da coinvolgere un elevato numero di utenze o che impattano potenzialmente su dati sensibili, giudiziari o comunque critici per l'Ente.

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.

12.1. 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 può essere risolta automaticamente o manualmente dal personale IT.

Qualora il personale IT, dall'analisi delle anomalie, ravvisi una potenziale debolezza o criticità nel sistema, deve darne comunicazione al responsabile IT che procederà alla relativa valutazione ed all'attivazione dell'eventuale intervento tecnico.

L'anomalia deve essere archiviata nel sistema di log automatico dello strumento tecnico impiegato per la sua gestione od evidenziata tramite ulteriori strumenti.

12.2. Gestione dell'incidente

Qualora venga rilevato un incidente l'utente IT deve comunicarlo al Responsabile IT.

Il Responsabile IT deve darne immediata comunicazione all'Ente che, ove l'incidente non sia risolvibile con risorse interne, provvederà a incaricare un Responsabile esterno per la sua gestione.

Il responsabile per la gestione dell'incidente deve identificarne le cause, definire l'intervento per la sua risoluzione, predisporre un piano di intervento che preveda le attività da porre in essere, le tempistiche e le 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 aggiornato l'Organo di Governo dell'Ente sullo stato degli interventi ed a relazionare a riguardo indicando:

- 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.

Qualora si verifichi una violazione dei dati personali (data breach), o della sicurezza che comporti 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 della protezione dei dati, ove individuato, ed all'Ente.

13. Entrata in vigore, riesame e aggiornamento

Il presente regolamento entra in vigore a partire dalla data di approvazione.

Il Regolamento può essere riesaminato ed aggiornato con cadenza periodica od al verificarsi di eventi che lo rendano necessario per garantirne l'idoneità, l'adeguatezza e l'efficacia.

14. Glossario

IT	Information Technology "Tecnologia dell'informazione": insieme di tecnologie utilizzate per l'archiviazione, la trasmissione e l'elaborazione di dati e informazioni attraverso l'uso di reti (reti aziendali, internet ecc.), elaboratori (PC, server, ecc.) ed attrezzature di telecomunicazione (datacenter, router, smartphone, tablet,ecc)
Responsabile IT	Responsabile della tecnologia dell'informazione: soggetto responsabile delle attività informatiche e dei sistemi informativi in uso nell'Ente
Personale IT	Soggetto addetto all'utilizzo di sistemi informativi all'interno dell'Ente
Amministratore di sistema	Soggetto deputato a garantire l'efficienza e la funzionalità del sistema informatico dell'Ente.
Criptatura	Conversione di dati da un formato leggibile ad un formato codificato che necessita di essere decriptato per poter essere letto od elaborato.
Distributed Denial	Attacco alla sicurezza informatica che mira a interrompere le attività aziendali.
DPO	Data Protection Officer. Soggetto responsabile per la protezione dei dati incaricato dal Titolare o dal Responsabile del trattamento.
DMZ (DeMilitarized Zone)	Area cuscinetto tra la rete interna e la rete esterna nella quale vengono limitati e controllati sia il traffico dati proveniente dall'esterno che quello interno.
Backup	Archiviazione di copia dei dati informatici su un dispositivo esterno.
DR	Disaster Recovery "Recupero dal disastro": Insieme di misure per ripristinare l'accesso e la funzionalità di infrastrutture IT in seguito a eventi naturali od umani (eventi calamitosi, guasti alle apparecchiature, attacchi informatici, furti, errori umani, ecc).
Log	File nel quale vengono conservate e registrate, in ordine cronologico, tutte le operazioni compiute da un software, un applicativo od un computer in autonomia od a seguito attività umana.
Software	Insieme delle componenti immateriali di un sistema informatico od elettronico di elaborazione (istruzioni di funzionamento di un programma codificate in linguaggio macchina o in linguaggio di programmazione -codice sorgente- memorizzate su uno o più supporti fisici, sotto forma di codice eseguibile).
Patch	File di aggiornamento software in grado di porre rimedio a specifiche vulnerabilità o migliorare la performance di un'applicazione oppure di correggere i malfunzionamenti e di risolvere i problemi e gli errori di programmazione che impediscono il corretto funzionamento di un programma o di un sistema operativo.
Firewall	Dispositivo per la sicurezza delle connessioni che controlla il flusso di dati in entrata ed in uscita tra reti diverse e blocca le connessioni pericolose per il sistema.
Rete wireless	Tecnologia di comunicazione tra sistemi o dispositivi informatici che permette di utilizzare la connessione Internet tramite onde radio ovvero senza l'utilizzo di cavi. Per estensione sono detti wireless i sistemi o dispositivi di comunicazione come i cellulari, le reti Wi-Fi e il Bluetooth.

NTP server	Network Time Protocol: protocollo per la sincronizzazione degli orologi dei computer all'interno di una rete
Client	Teminale che accede ai servizi o alle risorse di un server attraverso una rete informatica.
Server	Componente hardware o software (computer o programma) che fornisce i dati richiesti da altre componenti dette client attraverso una rete informatica
PROXY	Server che elabora e gestisce il traffico di informazioni tra più terminali interponendosi nel normale flusso di comunicazione tra i client e i server dei servizi web eliminando il collegamento diretto tra essi.
MALWARE	Software malevolo in grado di introdursi in un computer, in un dispositivo mobile o in una rete aziendale senza l'autorizzazione dell'utente con lo scopo di trafugare dati riservati, spiare le vittime o arrecare danni più o meno gravi al sistema informatico nel quale si introduce.
Lock	Procedura di sicurezza che consente l'accesso ad una risorsa condivisa in un ambiente multitasking ad un solo thread alla volta.
Lockout	Procedura di sicurezza che blocca l'accesso ad una risorsa condivisa in un ambiente multitasking dopo un certo numero di tentativi.
MAC address	Indirizzo che identifica in modo univoco una particolare interfaccia di rete di un dispositivo (un dispositivo dotato di Wi-Fi e Bluetooth è caratterizzato da due indirizzi MAC uno per l'interfaccia Wi-Fi e uno per l'interfaccia Bluetooth).
Multitasking	Capacità di un sistema operativo di eseguire più programmi contemporaneamente.
NAS	Network Attached Storage: dispositivo di archiviazione connesso alla rete informatica aziendale
Ridondanza	Tecnologia di archiviazione dei dati in due luoghi separati.
Services attack	Azione rivolta ad ingolfare le risorse di un sistema informatico per impedirne il funzionamento .
Thread	Unità di base o sequenza singola di esecuzione di un processo informatico.