Sistema Socio Sanitario

Regione Lombardia

ASST Valtellina e Alto Lario

Gestione Operativa: Next Generation EU - Qualità e Risk Management

**REGOLAMENTO**

# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

| | | |
|---|---|---|
| INDICE di REVISIONE | 00 | |
| DATA AGGIORNAMENTO | 08/02/2023 | |
| DESCRIZIONE MODIFICHE | Emissione | |
| **FASE** | **NOMINATIVO** | **Firma** |
| | S. Ruffoni - SC Affari Generali e Legali | |
| | A. Panese - Direttore SC Sistemi Informativi Aziendali - Responsabile della Transizione Digitale | |
| | C. Russo - Referente SIA - Cybersecurity e Piattaforme elettromedicali | |
| | A. Rossodivita - Direttore SC Gestione Operativa: Next Generation EU – Qualità e Risk Management - Responsabile della sicurezza delle informazioni | |
| | C. Paganoni - Incarico di Organizzazione Qualità e Risk Management - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management | |
| PRE-VERIFICA Data …….. | A. Faccinelli - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management | |
| | C. Paganoni - Incarico di Organizzazione Qualità e Risk Management - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management | |
| VERIFICA Data…… …. | R. Coppola – DPO aziendale | |
| | A. Andaloro - Responsabile Servizio Prevenzione e Protezione | |
| | A. Panese - Direttore SC Sistemi Informativi Aziendali - Responsabile della Transizione Digitale | |
| | R. Paroli - Direttore SC Gestione Acquisti (Provveditorato – Economato) | |
| | C. Zanesi – Direttore SC Gestione Tecnico Patrimoniale | |
| | S. Benedetti - Responsabile SS Trasparenza e Internal Auditing - SC Affari Generali e Legali | |
| | V. Berta – Responsabile per la tenuta del protocollo informatico della gestione dei flussi documentali e degli archivi | |
| | A. Rossodivita – Direttore SC Gestione Operativa: Next Generation EU – Qualità e Risk Management - Responsabile della sicurezza delle informazioni | |
| | C. Cecchini – Responsabile SS Ingegneria Clinica | |
| | E. Tanzi - Direttore SC Gestione e Sviluppo delle Risorse Umane | |
| | M. Piazza – Direttore Medico dei Presidi | |
| APPROVAZIONE DATA…….. | A. De Vitis - Direttore Amministrativo | |
| | G. Ardemagni – Direttore Sanitario | |
| | P. Formigoni - Direttore Socio Sanitario | |

| | | |
|---|---|---|
| VISTO | T. Saporito - Direttore Generale | |

# INDICE

Premessa ..... 3
Titolo I - Introduzione ..... 4
Titolo II - Obiettivi di sicurezza ..... 7
Titolo III - Organizzazione e responsabilità ..... 9
Titolo IV - Valutazione dei rischi ..... 10
Capo I - Rischi legati alla cybersecurity ..... 10
Capo II - Rischi legati alla supply chain ..... 12
Titolo V - Controlli di sicurezza ..... 13
Capo I - Sicurezza delle risorse informative ..... 13
Capo II - Sicurezza nell'ambito delle risorse umane ..... 16
Capo III - Sicurezza nelle relazioni con i soggetti terzi ..... 17
Capo IV - Sicurezza fisica e ambientale ..... 18
Capo V - Sicurezza delle attività operative ..... 20
Capo VI - Controllo degli accessi ..... 24
Sezione I - Accessi logici ..... 24
Capo VII - Acquisizione, sviluppo e manutenzione ..... 26
Capo VIII - Gestione degli incidenti rilevanti ai fini della sicurezza ..... 28
Capo IX - Gestione della continuità operativa ..... 29
Titolo VI - Controlli di conformità ..... 30
Capo I - Conformità ai requisiti cogenti e contrattuali ..... 30
Capo II - Conformità a standard internazionali e best practices ..... 31
Capo III - Riesame della sicurezza delle informazioni ..... 31
Titolo VII - Il sistema documentale ..... 32
Documenti di riferimento ..... 33
Allegato 1 – Piano attuativo ..... 35

# Premessa

La mission dell'Azienda Socio Sanitaria Territoriale della Valtellina e dell'Alto Lario (di seguito ASST) è quella di tutelare e promuovere la salute fisica e mentale della popolazione, attraverso l'erogazione dei LEA e degli eventuali livelli aggiuntivi definiti dalla Regione. La ASST assicura la continuità di presa in carico della persona nel proprio contesto di vita e affianca le persone croniche, fragili e le loro famiglie avviando un percorso culturale tra gli operatori che segni il passaggio dalla "cura" al "prendersi cura".

La ASST, consapevole del valore universale della salute, della sua natura di bene pubblico fondamentale e della rilevanza macroeconomica dei servizi sanitari pubblici, in linea con gli assi strategici e le priorità trasversali individuate nel Piano Nazionale di Ripresa e Resilienza (PNRR) [R16], ritiene che la digitalizzazione e l'innovazione dei propri processi e dei servizi erogati rappresentino un fattore determinante per la trasformazione del Paese.

D'altra parte, l'utilizzo pervasivo delle tecnologie dell'informazione e della comunicazione implica l'esposizione della Struttura Sanitaria a rischi cibernetici che devono essere opportunamente gestiti attraverso l'adozione di misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi, contribuendo in tal modo anche ad incrementare il livello comune di sicurezza del Paese, soprattutto alla luce del ruolo della Struttura Sanitaria come Operatore Essenziale nel quadro della normativa NIS [R9][R10].

A tal fine, la ASST adotta un approccio sistematico alla cybersecurity e più in generale alla sicurezza delle informazioni che indirizza un insieme organico e strutturato di misure di sicurezza logica, fisica, organizzativa e procedurale dedicate alla protezione dell'integrità, della riservatezza e della disponibilità delle informazioni e delle reti di comunicazione. L'implementazione di misure di sicurezza adeguate ed efficaci è, quindi, necessaria per garantire anche la sicurezza e la protezione dei dati personali contenuti all'interno del patrimonio informativo dell'ASST. L'approccio alla cybersecurity è, dunque, coerente con il modello organizzativo definito dalla ASST [R38] per assicurare la piena liceità e correttezza nei trattamenti dei dati personali effettuati.

In linea con tale approccio, la presente Politica declina un insieme di regole di base che indirizzano le strategie e le modalità di gestione della sicurezza delle informazioni della ASST, stabilendo:

- gli obiettivi di sicurezza;
- l'ambito di applicazione e i destinatari della Politica di Sicurezza;
- il modello organizzativo e gestionale definito per garantire la sicurezza delle informazioni;
- lo Statement formale e le contromisure logiche, fisiche o organizzative necessarie per la concreta realizzazione degli obiettivi di sicurezza prefissati;
- il sistema documentale inerente alla sicurezza delle informazioni.

# Titolo I - Introduzione

**Art. 1) Scopo del documento**

1. Il presente documento descrive la Politica per la Sicurezza delle Informazioni della ASST, intesa come l'insieme delle regole volte ad indirizzare una corretta gestione della sicurezza del Patrimonio Informativo, al fine di contenere i rischi di compromissione della riservatezza, dell'integrità e della disponibilità degli asset informativi, sia in un'ottica di tutela della missione istituzionale che di contrasto agli eventi accidentali o di natura criminosa.

**Art. 2) Campo di applicazione**

1. La presente Politica è valida per l'intera ASST e si applica a tutte le informazioni trattate in qualsiasi modo e qualsiasi formato, a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.
2. Le informazioni oggetto di protezione si riferiscono, a titolo esemplificativo e non esaustivo, ai seguenti ambiti:
   a) informazioni associate ai servizi istituzionali erogati e in via di sviluppo;
   b) know-how strategico;
   c) informazioni contabili e finanziarie;
   d) informazioni condivise con gli stakeholder, le Agenzie e le Amministrazioni governative;
   e) dati personali del personale della ASST, clienti e soggetti terzi, con riferimento al GDPR [R1], alla normativa nazionale attuativa [R2] ed ai Provvedimenti del Garante per la protezione dei dati personali;
   f) informazioni relative al pubblico che interagisce con la ASST;
   g) informazioni inerenti ai processi di procurement e di gestione dei progetti/contratti;
   h) informazioni legate alla gestione dei servizi e dei sistemi dedicati alla sicurezza ICT;
   i) informazioni trattate nell'ambito dei servizi essenziali di pertinenza della ASST [R9][R10][R11].
3. Le risorse cartacee ed informatiche utilizzate per l'elaborazione e la custodia delle informazioni, alle quali si indirizzano gli interventi di tutela, possono comprendere:
   a) documentazione tecnica o altri documenti contenenti le informazioni della ASST;
   b) procedure operative o di supporto;
   c) piattaforme hardware e software, incluse quelle che supportano i dispositivi elettromedicali;
   d) infrastrutture di rete e di telecomunicazione;
   e) banche dati;
   f) applicazioni gestionali e di supporto all'erogazione dei servizi;
   g) supporti di memorizzazione utilizzati per la conservazione dei dati.
4. Le Informazioni, le risorse informatiche, i supporti digitali e cartacei di archiviazione, costituiscono le cosiddette "Risorse Informative della ASST". Le Risorse Informative devono essere protette durante l'intero ciclo di vita fino al momento della loro dismissione.

5. Le regole di seguito descritte sono in vigore a partire dalla data di emissione del presente documento, ma per particolari ambiti, definiti nel presente documento, diverranno effettivi secondo un piano e relativo cronoprogramma di realizzazione, condiviso con i differenti responsabili delle parti interessate, e che verrà dettagliato in un modulo allegato.
6. Sono ammesse deroghe alle regole riportate nel presente documento, solo nei casi in cui ne sia valutato ed accettato il rischio derivante da parte della Direzione della ASST, con autorizzazione da parte della Direzione stessa.

**Art. 3) Definizioni e acronimi**

1. Ai fini dell'applicazione della presente Politica devono intendersi le seguenti definizioni:
   a) **Agenzia per la cybersicurezza nazionale**: l'Agenzia istituita a tutela degli interessi nazionali nel campo della cybersicurezza, di cui all'articolo 5 del decreto-legge 14 giugno 2021, n. 82 [R18].
   b) **Cybersecurity**: l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza.
   c) **Collaboratore esterno**: persona fisica che collabora con la ASST in forza di un contratto libero professionale.
   d) **CSIRT Italia**: il Computer Security Incident Response Team, di cui all'articolo 8 del decreto legislativo NIS [R10].
   e) **Decreto-legge:** il decreto-legge 14 giugno 2021, n. 82 [R18].
   f) **Decreto legislativo NIS**: il decreto legislativo 18 maggio 2018, n. 65 [R10].
   g) **Dato Personale**:dato personale ai sensi del GDPR [R1]: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
   h) **Direttiva NIS :** Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione [R9], recepita in Italia con il decreto legislativo 18 maggio 2018, n.65 [R10].
   i) **Operatore di Servizi Essenziali:** soggetto pubblico o privato, della tipologia di cui all'allegato II al decreto legislativo 18 maggio 2018, n. 65 [R10], che soddisfa i criteri di cui all'articolo 4, comma 2, de medesimo decreto.
   j) **Personale :** dipendente o assimilabile (es. contratti atipici).
   k) **Strategia nazionale di sicurezza cibernetica:** la strategia di cui all'articolo 6 del decreto legislativo NIS [R10].
   l) **Soggetti terzi:** Fornitori, consulenti, collaboratori esterni, partner che operano con la ASST in forza di un contratto.
   m) **Risorse Informative:** cfr. Art. 2) comma 4.

2. Ai fini dell'applicazione della presente Politica devono intendersi i seguenti acronimi:
   a) **ACN**:Agenzia per la cybersicurezza nazionale.
   b) **ASST:** Azienda Socio Sanitaria Territoriale della Valtellina e dell'Alto Lario.
   c) **AgID:** Agenzia per l'Italia Digitale.
   d) **BCP:** Business Continuity Plan.
   e) **CCNL:** Contratto Collettivo Nazionale di Lavoro.
   f) **CSIRT:** Computer Security Incident Response Team.
   g) **LEA:** Livelli Essenziali di Assistenza.
   h) **NIS:** Network and Information Security.
   i) **OSE:** Operatore di Sevizi Essenziali.
   j) **PNRR:** Piano Nazionale di Ripresa e Resilienza.
   k) **RAEE**: Rifiuti e Apparecchiature Elettriche ed Elettroniche

# Titolo II - Obiettivi di sicurezza

**Art. 4) Obiettivi per la sicurezza delle informazioni**

1. Considerando la missione istituzionale ed il quadro normativo di riferimento, la ASST si pone come obiettivo la salvaguardia di:
   a) la riservatezza delle informazioni, da attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle informazioni o la diffusione non controllata delle stesse;
   b) l'integrità delle informazioni, da attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
   c) la disponibilità delle informazioni, da attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse informatiche in tempi utili al compimento della propria missione.
2. Nello specifico la ASST deve, in via prioritaria:
   a) definire e applicare un processo di governance della sicurezza delle informazioni, che sia in grado di indirizzare le strategie di trattamento dei rischi in funzione dei cambiamenti derivanti dall'insorgere di nuovi scenari di minaccia, nuove tipologie di vulnerabilità, nuovi fattori di rischio derivanti anche dai cambiamenti organizzativi;
   b) definire e applicare un processo per l'analisi, la valutazione ed il trattamento dei rischi legati alla cybersecurity;
   c) prevedere, a tendere, l'integrazione tra il quadro di riferimento organizzativo e metodologico per l'analisi dei rischi legati alla cybersecurity e gli altri sistemi di gestione dei rischi della ASST, in modo da garantire una gestione e una valutazione unitaria dei rischi connessi ai servizi istituzionali della ASST;
   d) definire ed applicare un processo di gestione degli allarmi e degli incidenti di sicurezza informatica, che sia allineato e coerente con la procedura definita ed adottata dall'ASST per la gestione dei *data breach*;
   e) garantire al personale e ai soggetti terzi un'adeguata conoscenza e un grado di consapevolezza:
      - delle problematiche connesse alla sicurezza in termini di minacce, impatti e rischi derivanti da compromissioni della riservatezza, integrità e disponibilità del patrimonio informativo della ASST;
      - delle regole tecniche ed organizzative per l'utilizzo in sicurezza dei sistemi informativi della ASST;
      - delle procedure di rilevamento e segnalazione di eventi anomali o sospette violazioni della sicurezza informatica;
      - della normativa applicabile in materia di protezione dei dati personali [R1] e delle relative implicazioni, nonché delle modalità di applicazione delle misure previste dalla normativa nonché dalle procedure/istruzioni contenute all'interno del Modello Organizzativo Privacy dell'ASST;

f) garantire la conformità ai requisiti cogenti derivanti da normative di legge, dagli standard internazionali e dalle principali best practice di settore;

g) garantire il rispetto della politica per la sicurezza delle informazioni adottata dalla ASST.

# Titolo III - Organizzazione e responsabilità

**Art. 5) Organizzazione e responsabilità per la sicurezza delle informazioni**

1. L'organizzazione è funzionale all'individuazione delle politiche dirette alla gestione e al controllo delle misure di sicurezza adottate e si concretizza nella definizione di ruoli, funzioni e responsabilità che concorrono alla realizzazione ed alla gestione del sistema di sicurezza delle informazioni, tenendo conto anche del ruolo della ASST come infrastruttura critica nel settore di riferimento e all'interno della filiera produttiva.
2. La ASST si impegna a definire specifici ruoli e responsabilità per la sicurezza delle informazioni, ad attribuirli alle diverse strutture organizzative interne e a comunicarli affinché siano pienamente compresi ed attuati.
3. I compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset della ASST.
4. Nella definizione delle responsabilità associate ai ruoli devono essere previste le attività di gestione dei contatti con le autorità nazionali ed internazionali e con gruppi specialistici e associazioni professionali pertinenti alla sicurezza delle informazioni, nonché le attività di gestione della sicurezza delle informazioni nell'ambito dei progetti.

# Titolo IV - Valutazione dei rischi

**Art. 6) Scenari di minaccia**

1. Il progressivo e crescente ricorso alle tecnologie digitali delinea nuovi scenari di minaccia alla cybersecurity che potrebbero compromettere il corretto svolgimento dei servizi, l'integrità degli asset infrastrutturali e determinare violazioni dei diritti e delle libertà delle persone fisiche.
2. D'altra parte, le filiere di approvvigionamento (supply chain) possono a loro volta introdurre nuove minacce e talvolta aumentare il livello di complessità delle azioni di contrasto alle minacce, nonché rallentarne i tempi di attuazione.
3. La ASST ritiene pertanto fondamentale realizzare un processo di valutazione dei rischi legati alla cybersecurity (di seguito anche rischi cyber) ed alla supply chain, individuando allo stesso tempo le opportune procedure di gestione e riduzione di tali rischi.

# Capo I - Rischi legati alla cybersecurity

**Art. 7) Principi generali**

1. Il processo di valutazione dei rischi cyber e la corrispondente metodologia, affinché siano allineati ai principali standard di riferimento e consentano di ottenere risultati utili, affidabili e rappresentativi della realtà del contesto analizzato, devono soddisfare i seguenti principi generali:
   a) **Ripetibilità e riproducibilità** - Uno dei risultati del processo di valutazione del rischio cyber è la misurazione del rischio. Tale operazione richiede di essere ripetibile, vale a dire, a parità di ogni altra condizione, si devono ottenere i medesimi risultati, anche in tempi successivi. Da qui la necessità di documentare il metodo utilizzato e almeno le principali assunzioni e semplificazioni.
   b) **Comprensibilità** - I criteri adottati nell'espressione dei parametri che compongono il rischio (probabilità di accadimento, valore delle informazioni, etc.) e i risultati prodotti devono essere logici e trasparenti, al fine di consentire il riutilizzo dei risultati nella ripetizione del processo di valutazione del rischio cyber.
   c) **Condivisione** - Il processo di valutazione del rischio cyber deve essere stabilito, gestito e concordato tra i responsabili della ASST (c.d. stakeholder) ed i valori attribuiti alle informazioni devono essere condivisi tra le diverse Strutture della ASST interessate.
   d) **Coerenza** - I valori attribuiti alle informazioni devono essere coerenti con quanto stabilito dalle politiche di sicurezza di alto livello della ASST.
   e) **Riutilizzabilità** - I risultati del processo di valutazione del rischio cyber, intermedi o finali, devono poter essere riutilizzabili nel caso in cui l'attività vada ripetuta a seguito di variazioni delle condizioni (valori delle informazioni, minacce, vulnerabilità, etc.) che ne hanno determinato l'esecuzione, anche al fine di realizzare economie di scala. Inoltre, è importante evidenziare che la revisione dell'analisi dei rischi contribuisce all'attuazione del concetto di miglioramento continuo e della sua misurazione. Se necessario, i parametri che definiscono le minacce, così come le vulnerabilità, possono essere ampliati in funzione delle variazioni del contesto di analisi, delle risorse impiegate e delle terze parti che entrano in contatto, per finalità diverse, con l'ambito dell'analisi.

f) **Fattibilità in termini temporali** - Le attività correlate al processo di valutazione del rischio cyber devono fornire i risultati in tempi utili, legati ad esempio, al livello di criticità del servizio oggetto di analisi ed al suo ciclo di vita, oppure commisurati con il livello di rischio e/o con il budget allocato secondo anche le regole di sistema.

g) **Adeguatezza al livello di consapevolezza dell'Organizzazione** - La complessità di una metodologia per la valutazione del rischio cyber deve essere adeguata al livello di consapevolezza esistente nella ASST sui temi relativi alla sicurezza delle informazioni, per evitare gli insuccessi derivanti dall'introduzione di sistemi di gestione e processi non recepiti e lasciati allo stato di evento occasionale, avulso dalla cultura interna alla ASST. In considerazione della complessità di tale politica e della sua applicabilità, si ritiene che tale politica e l'adeguamento del livello di consapevolezza richiederà un percorso di implementazione, attraverso la redazione di un piano attuativo dedicato, della durata stimata di 5 anni, dall'entrata in vigore del presente documento.

**Art. 8) Processo**

1. Il processo di valutazione del rischio cyber, in linea con quanto previsto dai principali standard ISO applicabili in materia [R24][R28] e con il Framework Nazionale per la Cybersecurity e la Data Protection [R20], deve essere costituito da un insieme di attività ben definite, da compiersi in sequenza ordinata, nell'ambito delle seguenti macro-fasi:

   a) **Context Establishment:** identificazione dell'ambito, dei confini e dell'organizzazione a supporto del processo di valutazione del rischio cyber;

   b) **Risk Assessment:** analisi e valutazione del rischio, che a sua volta deve prevedere le seguenti attività:

      - identificazione e documentazione delle vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione;
      - identificazione e valutazione delle minacce, sia interne che esterne e le relative probabilità di accadimento;
      - identificazione e valutazione dei potenziali impatti sulla mission istituzionale della ASST;
      - valutazione del rischio in base a quanto emerso dai suddetti punti.

      Ai fini della identificazione e valutazione delle minacce e delle vulnerabilità la ASST deve organizzarsi in modo da ricevere informazioni su minacce, vulnerabilità ed altri dati configurabili come Cyber Threat Intelligence da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing).

   c) **Risk Treatment:** definizione delle strategie per la gestione del rischio e definizione delle modalità operative per l'implementazione delle misure di sicurezza adeguate alla copertura dei rischi rilevati, che a sua volta deve prevedere le seguenti attività:

      - identificazione e comunicazione del livello di rischio tollerato;
      - definizione strategia di trattamento del rischio, con identificazione e prioritizzazione delle misure tecniche ed organizzative necessarie per contenere il rischio valutato entro la soglia di accettazione definita dalla ASST o soddisfare requisiti di compliance normativa non ancora pienamente soddisfatti.

2. Una caratteristica fondamentale dell'attività di valutazione del rischio cyber è che deve configurarsi come un processo continuo, da cui desumere le azioni da implementare per una

gestione del rischio consapevole, adeguata ai valori da proteggere (in termini di informazioni o servizi erogati dal sistema informativo) ed in linea, sul piano temporale, con i mutamenti ambientali e tecnologici.

### Art. 9) Rischio tollerato

1. Con riferimento al rischio cyber tollerato, la ASST, tenendo conto del ruolo dell'Organizzazione come Operatore Essenziale ai sensi della Direttiva NIS [R9] e dei rischi specifici presenti nel settore di appartenenza, ha individuato in un livello basso su una scala di valori a tre livelli (Basso, Medio, Alto), la soglia di rischio accettabile, rispetto alla riservatezza, alla integrità e alla disponibilità delle informazioni.
2. Il livello di rischio tollerato implica che sugli asset esposti a livelli di rischio inferiori o uguali a tale soglia, non sia richiesta l'implementazione di misure di sicurezza specifiche ulteriori rispetto a quanto previsto dalle politiche adottate dall'Ente, dai requisiti normativi e contrattuali e dalle best practice internazionali.
3. Il rispetto delle politiche e dei requisiti normativi, infatti, risulta indipendente dalle attività di analisi del rischio e definisce quindi un insieme minimo di misure di sicurezza.
4. Nell'ambito delle specifiche analisi del rischio su servizi o applicazioni possono essere stabilite soglie di rischio accettato diverse da quelle esplicitate nel presente documento, solo in caso di deroga autorizzata dalla ASST per comprovate esigenze.

# Capo II - Rischi legati alla supply chain

### Art. 10) Processi di gestione del rischio inerenti alla catena di approvvigionamento cyber

1. La ASST deve inoltre definire ed implementare i processi di gestione del rischio inerenti alla catena di approvvigionamento cyber.
2. A tal fine i soggetti terzi che forniscono sistemi informatici, componenti e servizi ICT devono essere identificati, prioritizzati e valutati regolarmente da parte della ASST tramite attività di audit, verifica, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali (cfr. Art. 26).
3. Inoltre, i suddetti soggetti terzi devono essere opportunamente coinvolti nelle attività di pianificazione e verifica della risposta e del ripristino agli incidenti aventi impatto sulla sicurezza e sulla continuità operativa dei servizi erogati dalla ASST (cfr. Capo VIII - Capo IX - ).

# Titolo V - Controlli di sicurezza

**Art. 11) Controlli di sicurezza delle informazioni**

1. La ASST ritiene che la sicurezza delle informazioni si ottenga implementando un insieme adeguato e coerente di controlli organizzativi e tecnologici.
2. Di seguito sono formalmente declinati i controlli che costituiscono la presente politica, da attuare per il raggiungimento degli obiettivi di sicurezza definiti dalla ASST (cfr. Titolo II - ), in base al contesto specifico di riferimento.
3. I controlli sono organizzati in funzione dell'ambito della sicurezza delle informazioni che indirizzano.
4. Tale politica richiederà per l'attuazione la realizzazione di un piano strategico dedicato di attuazione della durata complessiva stimata di 5 anni, nell'ambito del quale verranno declinate tempistiche, interventi di implementazione crescenti e progressivi, ruoli e responsabilità di realizzazione secondo un cronoprogramma predefinito.

# Capo I - Sicurezza delle risorse informative

**Art. 12) Risorse informative**

1. Tutte le Risorse Informative della ASST (cfr. Art. 2) costituiscono un valore strategico per l'organizzazione e come tali devono essere adeguatamente protette.
2. Nell'ambito delle Risorse Informative, l'informazione assume un ruolo d'importanza primaria costituendo una risorsa critica immateriale, necessaria ai processi di pianificazione, organizzazione, esecuzione e controllo delle attività condotte dalla ASST.

**Art. 13) Inventario degli asset**

1. L'inventario delle risorse informative è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, rinnovare le licenze e programmare gli investimenti in tecnologie dell'informazione.
2. L'inventario deve comprendere:
   a) **Informazioni:** database e archivi cartacei, documentazione di sistema, manuali per l'utente, materiale per l'addestramento, procedure operative o di supporto, piani di continuità, ecc.;
   b) **Risorse software:** software di base ed applicativo, strumenti di sviluppo, programmi di utilità, ecc.;
   c) **Risorse hardware:** apparecchiature informatiche (ad es. server fisici e virtuali, client fissi e portatili, monitor, sistemi di backup e restore, ecc.), apparecchiature di comunicazione (ad es. router, fax, segreterie telefoniche, ecc.), supporti magnetici (ad es. nastri e dischi), altre apparecchiature tecniche (ad es. alimentazioni elettriche, unità di climatizzazione, ecc.);
   d) **Sistemi informativi esterni** all'organizzazione utilizzati nell'ambito della ASST (ad es. cloud);
   e) **Flussi di dati e comunicazioni** inerenti all'organizzazione;

f) **Locali:** i luoghi fisici ove sono custodite le informazioni, le risorse software e hardware e dove vengono effettuate le elaborazioni;

g) **Capitale umano:** personale e soggetti terzi che operano presso la ASST.

3. A tal fine deve essere predisposto e mantenuto aggiornato un inventario delle principali Risorse Informative che includa tutti i suddetti asset. Inoltre, a tali asset devono essere associati i relativi servizi erogati dalla ASST, con specifica indicazione di quelli ritenuti essenziali ai sensi della Direttiva NIS [R9] e delle Linee Guida emesse dall'Autorità NIS-Settore Salute [R11].
4. Infine, devono essere identificati e catalogati tutti i trattamenti di dati personali effettuati dalla ASST ai sensi del GDPR [R1] (Registri dei trattamenti di dati personali).
5. Tutte le Risorse Informative sono di proprietà della ASST, a cui è riservato ogni diritto ai sensi della normativa vigente sulla Protezione del diritto d'autore, laddove applicabile.
6. La riproduzione, la pubblicazione e la distribuzione, totale o parziale, delle Risorse Informative sono espressamente vietate in assenza di una autorizzazione scritta da parte del proprietario.
7. L'inventario degli asset già iniziato, diversificato per l'aspetto informatico e quello cartaceo, richiederà per la completa realizzazione dell'intero processo un arco temporale non inferiore ai 5 anni (vedasi piano attuativo allegato).

**Art. 14) Utilizzo degli asset**

1. Il personale utilizza le Risorse Informative di proprietà della ASST nei limiti dell'autorizzazione assegnata e per esclusive finalità lavorative.
2. Tale utilizzo deve sempre ispirarsi ai principi di diligenza, correttezza e riservatezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto professionale, in coerenza con le vigenti normative, e tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.
3. La ASST, ammette l'uso degli strumenti informatici, ed in particolare di Internet, per motivi personali soltanto in caso di urgenza e comunque non in modo ripetuto e per periodi di tempo brevi, e in ogni caso sempre nel rispetto del principio di riservatezza e delle esigenze di funzionalità della rete e di semplificazione dei processi lavorativi.
4. La ASST perseguirà a norma di legge e del vigente contratto di lavoro, il personale che utilizza in modo non appropriato i sistemi di elaborazione delle informazioni, poiché l'eventuale esposizione al rischio impedirebbe alla ASST il corretto svolgimento delle proprie attività istituzionali ed il rispetto delle normative cogenti applicabili.
5. A tal fine devono essere predisposte idonee istruzioni per il personale, contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche derivanti, in caso di inosservanza.

**Art. 15) Classificazione e trattamento delle informazioni**

1. Le informazioni trattate nell'ambito delle attività della ASST devono essere tutelate e gestite sulla base del loro valore in termini di impatti derivanti dalla perdita della disponibilità, integrità e riservatezza delle stesse.
2. Tutte le informazioni trattate dalla ASST devono essere classificate attribuendo alle stesse un grado di criticità utile a determinarne il livello di protezione.

3. La protezione deve riguardare tutte le fasi connesse alla gestione dell'informazione: generazione, raccolta, classificazione, emissione, oscuramento ove previsto dalle norme (cfr. ad esempio [R13][R14] e s.m.i.), ricezione, custodia, divulgazione, consultazione, riclassificazione, modifica, conservazione e distruzione.
4. A tal fine, devono essere predisposte dalla ASST adeguate politiche contenenti, in conformità alle esigenze istituzionali ed alla normativa vigente in materia di tutela del trattamento dei dati personali [R1]:
   a) i criteri per la classificazione delle informazioni;
   b) le misure minime di sicurezza da adottare per il trattamento delle informazioni classificate e la relativa etichettatura.

**Art. 16) Assegnazione di priorità agli asset**

1. Gli asset della ASST (cfr. Art. 13) devono essere prioritizzati in base alla classificazione (cfr. Art. 15), criticità e valore per la mission dell'organizzazione, delle informazioni da essi trattate.
2. Inoltre, devono essere identificate e rese note le interdipendenze e le funzioni fondamentali per la fornitura di servizi critici.

**Art. 17) Utilizzo di supporti e dispositivi informatici della ASST per la memorizzazione**

1. La memorizzazione delle informazioni deve essere effettuata utilizzando le applicazioni istituzionali preposte (es. Sharepoint, OneDrive) ed è pertanto necessario limitare la memorizzazione di informazioni su supporti e dispositivi informatici della ASST (dischi locali del PC, memorie esterne, ecc.).
2. È comunque necessario regolamentare la memorizzazione di informazioni su supporti e dispositivi informatici della ASST (dischi locali del PC, memorie esterne, ecc.) prevedendo un processo formale di autorizzazione nel caso di memorizzazione di dati personali ai sensi del GDPR [R1] o critici della ASST.
3. Inoltre, i supporti e i dispositivi informatici della ASST per la memorizzazione, incluse le memorie esterne (es. cd rom, dvd, hard disk portatili, chiavi USB), devono essere protetti dai rischi di accesso non autorizzato e/o manomissioni, in funzione della classificazione delle informazioni in essi contenuti.

**Art. 18) Utilizzo di supporti e dispositivi personali**

1. Non è consentito l'utilizzo di supporti e dispositivi personali ai fini dello svolgimento dell'attività lavorativa, fatto salvo situazioni specifiche che dovranno essere di volta in volta autorizzate dalla ASST valutandone il rischio derivante.

**Art. 19) Lavoro da remoto**

1. La ASST è consapevole che il lavoro da remoto può risultare fondamentale per favorire l'efficienza e l'efficacia delle attività in particolari situazioni aziendali e sociosanitarie.
2. Tuttavia, tale modalità può comportare rischi anche significativi per la sicurezza delle informazioni della ASST e pertanto deve essere opportunamente regolamentato, nel rispetto di quanto consentito dalla legge vigente e dai contratti di lavoro.

# Capo II - Sicurezza nell'ambito delle risorse umane

**Art. 20) Individuazione del personale**

1. Tutto il personale della ASST ed i collaboratori esterni, con particolare riferimento a quelli destinati a ricoprire ruoli di gestione della sicurezza, devono essere attentamente individuati, in funzione delle esigenze istituzionali della ASST e sulla base di criteri di affidabilità e competenza professionale.
2. Una volta individuato il personale si procederà ad assegnare i compiti al personale dedicato alla sicurezza delle informazioni, oltre alla struttura organizzativa di appartenenza, specifici ruoli operativi e profili professionali, previo adeguato percorso formativo ad hoc.

**Art. 21) Responsabilità del personale e dei collaboratori esterni**

1. Tutto il personale e i collaboratori esterni devono essere informati delle proprie responsabilità, anche giuridiche, derivanti da violazioni, frodi o dall'utilizzo improprio delle Risorse Informative della ASST, nonché da uno scorretto trattamento delle informazioni e dei dati personali.
2. I rapporti interpersonali ed i comportamenti, a tutti i livelli organizzativi, devono essere improntati a principi di onestà, correttezza, trasparenza, riservatezza, imparzialità, diligenza, lealtà e reciproco rispetto (per il personale si rimanda al Contratto Collettivo Nazionale di Lavoro, al Regolamento recante codice di comportamento dei dipendenti pubblici [R32], ai codici deontologici dei rispettivi ordini professionali ed al Regolamento per i procedimenti disciplinari relativi al personale dipendente del comparto della dirigenza della ASST [R37], mentre per i collaboratori esterni ai contratti individuali).

**Art. 22) Sensibilizzazione e formazione**

1. Tutto il personale ed i collaboratori esterni devono essere adeguatamente informati e sensibilizzati in merito alle politiche e alle procedure operative di sicurezza pertinenti alla propria attività lavorativa.
2. In particolare, devono essere definiti, erogati e aggiornati piani formativi mirati ad accrescere il grado di consapevolezza e di sensibilizzazione sugli obiettivi di sicurezza prefissati e sulle principali problematiche di sicurezza delle informazioni.
3. I piani di formazione devono prevedere un approfondimento specifico su:
   a) politiche, procedure e linee guida di sicurezza adottate dalla ASST;
   b) ruoli organizzativi previsti per la gestione delle tematiche di sicurezza delle informazioni, responsabilità del personale coinvolto e principali implicazioni di eventuali non conformità sulla sicurezza delle risorse della ASST;
   c) principali tematiche e controlli di sicurezza delle informazioni, inclusa la cybersecurity.

**Art. 23) Cessazione e variazione del rapporto di lavoro**

1. Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o variazione del rapporto di lavoro devono essere definiti, comunicati al personale ed ai collaboratori esterni e resi effettivi.

# Capo III - Sicurezza nelle relazioni con i soggetti terzi

**Art. 24) Controlli generali**

1. Tutti i soggetti terzi devono essere informati delle proprie responsabilità, anche giuridiche, derivanti da violazioni della sicurezza o dall'utilizzo improprio delle Risorse Informative della ASST, qualora l'attività individuata possa comportare l'accesso a tali risorse.
2. È necessario garantire la sicurezza delle Risorse Informative accedute ed utilizzate anche dai soggetti terzi che a qualsiasi titolo, svolgono, anche temporaneamente, attività di lavoro per la ASST.
3. La ASST, come evidenziato nelle Linee Guida per la sicurezza nel procurement ICT [R31], è consapevole che i soggetti terzi in relazione alla natura dei servizi offerti, possono accedere al patrimonio informativo della ASST, introducendo potenziali rischi cyber in grado di vanificare, o comunque rendere meno efficaci, le misure prese dalla ASST per tutelare il proprio patrimonio informativo. Risulta pertanto fondamentale definire ed attuare procedure per garantire la sicurezza delle informazioni in relazione all'approvvigionamento di beni e servizi informatici (procurement ICT) che indirizzino tutte le fasi di approvvigionamento (prima, durante e dopo).
4. È necessario garantire la sicurezza delle Risorse Informative rese disponibili all'utilizzo da parte di soggetti terzi ai fini dell'esecuzione degli specifici obblighi contrattuali e nei limiti dell'autorizzazione assegnata.
5. A tal fine, devono essere predisposte:
   a) adeguate politiche e procedure contenenti i criteri e le modalità per la gestione delle Risorse Informative da parte dei soggetti terzi, in conformità alle esigenze istituzionali ed alle normative vigenti. Tali politiche e procedure devono risultare adeguate rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle Risorse Informative della ASST;
   b) idonee istruzioni contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche, derivanti in caso di inosservanza.
   c) Il miglioramento e potenziamento di tali politiche e procedure richiederà un arco temporale stimato di 3 anni (vedasi piano attuativo allegato).

**Art. 25) Clausole Contrattuali**

1. Devono essere previste specifiche clausole per garantire la riservatezza e la non-divulgazione delle informazioni della ASST accedute ed utilizzate dai soggetti terzi, secondo quanto previsto dalle normative vigenti.
2. Gli accordi con i soggetti terzi devono necessariamente contemplare tutti i requisiti necessari ad assicurare la protezione delle Risorse Informative della ASST e devono indirizzare l'intera catena di approvvigionamento a garanzia del mantenimento della sicurezza delle informazioni in tutte le fasi.
3. Inoltre, i soggetti terzi devono essere informati sulle politiche, le procedure e le istruzioni di sicurezza della ASST relativamente al tipo di attività previste dal contratto.
4. Il miglioramento e potenziamento richiederà un arco temporale stimato di 3 anni (vedasi piano attuativo allegato).

### Art. 26) Monitoraggio, revisione e gestione del cambiamento dei servizi delle terze parti

1. I servizi delle terze parti devono essere regolarmente monitorati, riesaminati e verificati al fine di rilevare scostamenti rispetto agli accordi contrattuali nonché gestire eventuali cambiamenti alla fornitura di tali servizi (in occasione ad esempio di interventi migliorativi, cambiamenti tecnologici o delle politiche e delle procedure di sicurezza, rivalutazione dei rischi).
2. Il miglioramento e potenziamento richiederà un arco temporale stimato di 3 anni (vedasi piano attuativo allegato).

### Art. 27) Sicurezza delle informazioni per l'utilizzo dei servizi cloud

1. Devono altresì essere definite politiche specifiche e relativi processi atti ad indirizzare e gestire la sicurezza delle informazioni lungo tutto il ciclo di vita dei servizi cloud.

# Capo IV - Sicurezza fisica e ambientale

### Art. 28) Protezione da minacce di tipo fisico ed ambientale

1. Tutte le Risorse Informative, cartacee ed informatiche, della ASST devono essere protette dai rischi di accesso non autorizzato, sottrazione, manomissioni e danneggiamento derivanti da minacce di tipo fisico ed ambientale.
2. Saranno progettati ed implementati sistemi di sicurezza fisica per la protezione delle aree, degli uffici, delle stanze e degli impianti dai danni derivanti da incendi, allagamenti, esplosioni ed altre forme di disastro naturale o umano, in coerenza con le risorse tecnico-strutturali, economiche e logistiche aziendali.
3. I sistemi di sicurezza adottati devono essere regolarmente verificati e manutenuti.
4. Devono essere predisposte idonee procedure organizzative per la regolamentazione ed il controllo dell'accesso ai sistemi informatici da parte del personale e dei soggetti terzi autorizzati alla gestione/manutenzione degli stessi.
5. Il miglioramento e potenziamento richiederà per la realizzazione un arco temporale di 5 anni (vedasi piano attuativo allegato).

### Art. 29) Sicurezza delle aree

1. Il perimetro di sicurezza delle aree contenenti le informazioni critiche e le strutture di elaborazione delle informazioni deve essere chiaramente definito e controllato.
2. Quando non presidiate, le aree devono essere tenute chiuse e controllate periodicamente.

### Art. 30) Controllo degli accessi fisici

1. Tutte le risorse informative devono essere ubicate prevalentemente in edifici con accesso a personale preventivamente autorizzato. L'accesso fisico a tali strutture deve essere controllato e consentito solo al personale e agli eventuali soggetti terzi e visitatori preventivamente identificati ed autorizzati, solo per i compiti specifici e limitati alle attività di competenza.
2. Il personale che fornisce servizi di supporto e di manutenzione è autorizzato all'accesso nelle aree laddove necessario e in maniera limitata (anche temporalmente).
3. I diritti di accesso devono essere regolarmente verificati e revocati al personale ed ai soggetti terzi che lasciano gli incarichi per i quali era previsto l'ingresso alle aree stesse.

4. A tal fine:
   a) devono essere predisposte idonee procedure per la regolamentazione ed il controllo degli accessi alle aree e ai locali della ASST;
   b) devono essere previste “aree ad accesso ristretto”, ove necessario alla luce dei potenziali rischi per la sicurezza delle informazioni, dove l’ammissione è consentita solo in presenza di personale autorizzato (ad es. locali ove risiedono i sistemi server e le apparecchiature di rete, quelli dedicati alla medicina nucleare e risonanza magnetica, laboratori di analisi, archivi cartelle cliniche, ecc.).

**Art. 31) Sicurezza degli uffici, delle stanze e degli strumenti di lavoro**

1. Gli uffici e le stanze devono essere protetti in funzione della classificazione delle risorse informative ivi trattate e custodite (cfr. Art. 15).
2. L’accesso agli uffici ed alle stanze deve essere consentito solo al personale autorizzato, ai soggetti terzi ed ai visitatori preventivamente identificati.
3. Gli strumenti di lavoro devono essere fisicamente protetti dai rischi di accesso non autorizzato e da conseguenti manomissioni o furti.
4. Saranno predisposte idonee procedure organizzative per la regolamentazione ed il controllo degli accessi agli strumenti da parte del personale e dei soggetti terzi autorizzati alla gestione/manutenzione degli stessi.

**Art. 32) Lavorare in aree sensibili**

1. Devono essere progettati ed implementati idonei sistemi di sicurezza fisica per la protezione ed il controllo delle aree sensibili, qualora identificate.
2. Devono essere definite procedure organizzative per la gestione dell’accesso alle aree sensibili da parte del personale, dei soggetti terzi ed eventuali visitatori.
3. Devono essere altresì definite, linee guida ed istruzioni per la regolamentazione delle attività lavorative e dell’utilizzo delle risorse informative all’interno delle aree sensibili. Tali attività necessiteranno per la realizzazione completa di un arco temporale non inferiore a 5 anni (vedasi piano attuativo allegato).

**Art. 33) Sicurezza delle aree di carico e scarico**

1. Le aree di carico e scarico dei materiali, laddove presenti, devono essere controllate ed isolate dagli ambienti operativi e di elaborazione delle informazioni.
2. Le porte di accesso alle aree di carico e scarico dovranno essere sorvegliate e se possibile allarmate.
3. L’accesso alle suddette aree deve essere limitato al personale ed ai soggetti terzi previamente identificati e autorizzati.
4. Tutto il materiale in uscita ed in arrivo deve essere sempre registrato all'entrata. Il materiale in arrivo deve essere sempre possibilmente esaminato prima di venire trasportato dall'area di carico e scarico al punto di utilizzo.

**Art. 34) Equipaggiamento di sicurezza**

1. Tutti i locali della sala server aziendali della ASST devono essere dotati di equipaggiamento di sicurezza come rilevatori di fumo e di fiamme, allarmi antincendio, controllo delle

temperature, attrezzature per l'estinzione di incendi, uscite di sicurezza, sistemi antiallagamento e sistemi di protezione dalle interferenze nella fornitura elettrica.

2. Tali equipaggiamenti devono essere controllati periodicamente per accertarne lo stato di conservazione e l'efficienza seguendo le istruzioni dei costruttori e dei responsabili preposti.
3. Tutte le informazioni sulla collocazione degli equipaggiamenti devono essere riportate su planimetrie opportunamente dislocate nelle aree comuni.
4. Tutto il personale e gli eventuali soggetti terzi devono essere istruiti all'uso di tali equipaggiamenti. Le procedure di emergenza devono essere documentate e regolarmente testate.

**Art. 35) Sicurezza del cablaggio**

1. È necessario proteggere il cablaggio da minacce di tipo fisico, ambientale e organizzativo.
2. Il cablaggio deve essere collocato in posizione priva di rischi dovuti a perdita di fluidi e/o disturbi elettromagnetici indotti da altri sistemi e tale da consentirne un'agevole e sicura manutenzione.
3. Deve essere garantita la protezione fisica dei cavi di dorsale, dei cavi orizzontali e dei locali tecnici.

# Capo V - Sicurezza delle attività operative

**Art. 36) Procedure operative e responsabilità**

1. Le procedure operative inerenti ai processi di gestione dei sistemi informatici devono essere documentate, manutenute e rese facilmente disponibili a tutto il personale incaricato di attuarle.
2. Qualsiasi modifica inerente ai sistemi e agli strumenti di gestione delle informazioni deve essere autorizzata, controllata e documentata.
3. Le responsabilità del controllo devono essere affidate a strutture o a personale esterno alle aree operative, onde ridurre le opportunità di modifiche non autorizzate o accidentali e manomissioni delle risorse informative della ASST.
4. Gli ambienti di sviluppo, di produzione e test devono essere separati al fine di ridurre al minimo i rischi di accessi o modifiche non autorizzate o anche accidentali dei relativi sistemi informativi.
5. La realizzazione di queste attività necessiterà un arco temporale di 3 anni (vedasi piano attuativo allegato).

**Art. 37) Protezione da malicious software**

1. L'integrità delle informazioni e delle risorse informatiche deve essere preservata dalla possibile compromissione da parte di software malevolo (ad esempio virus, worm, trojan horses).
2. Al riguardo è necessario definire:
   a) una politica di formazione ed informazione del personale e degli eventuali soggetti terzi sui danni potenziali arrecati alle Risorse Informative, legati all'introduzione di software malevolo;

b) idonee contromisure per l'individuazione di software malevolo nei sistemi informatici, nonché per il ripristino delle risorse eventualmente danneggiate. In tal senso, le postazioni di lavoro devono disporre almeno di un sistema antivirus aggiornato allo stato dell'arte.

c) I programmi antivirus devono essere gestiti e controllati in maniera tale da assicurarne una capillare diffusione ed un frequente aggiornamento.

d) Devono essere definite idonee contromisure atte a gestire gli eventi dannosi (isolamento, ripristino) ed a fornire supporto agli utenti coinvolti.

**Art. 38) Software non autorizzato**

1. Deve essere vietato l'utilizzo di software non espressamente autorizzati. Tutti i software installati sui sistemi informativi devono essere conformi ai termini delle licenze (vincoli d'uso) ed utilizzato per esclusive finalità lavorative.
2. Al riguardo è necessario impedire l'incauto prelievo di software e di file da computer remoti o la loro installazione non autorizzata in computer della ASST.
3. Tutto il personale deve essere reso consapevole dei danni potenziali arrecati alle Risorse Informative dall'introduzione di software non autorizzati, diversi da quelli standard in dotazione.
4. Devono essere definite idonee politiche e procedure di sicurezza e previsti strumenti per la prevenzione e l'individuazione di software non autorizzato nel sistema informatico nonché per il ripristino delle risorse eventualmente danneggiate.

**Art. 39) Back-up**

1. Per i sistemi ancora presenti sui Data Center aziendali devono essere previste, anche in conformità alle normative vigenti, adeguate politiche e procedure di back-up per preservare l'integrità e garantire la disponibilità delle informazioni (ad esempio in caso di manomissioni, atti vandalici, contaminazione da virus, perdita o distruzione anche involontaria).
2. Le procedure devono riguardare la verifica della corretta esecuzione dei back-up, il mantenimento di un elenco delle copie effettuate, l'archiviazione sicura, i criteri ed i tempi per la conservazione dei supporti di memorizzazione (dischi, nastri ecc.), i meccanismi e le modalità per la cancellazione sicura delle informazioni in caso di distruzione, smaltimento o riutilizzo dei supporti.
3. Laddove il back-up venga effettuato localmente nell'ambito dell'ufficio devono essere impartite al personale e agli eventuali soggetti terzi, le idonee istruzioni tecniche ed organizzative. Tali istruzioni devono indicare gli strumenti e le modalità con cui effettuare le copie di sicurezza, l'elenco delle banche dati e degli archivi per i quali è richiesta la copia, la sequenza temporale e la finestra operativa per garantire che i dati copiati siano tra loro congruenti.
4. Si stima, in termini di adeguamento di quanto già esistente, la completa realizzazione di queste attività in un arco temporale non inferiore ai 2 anni (vedasi piano attuativo allegato). Si precisa che tali attività sono già in corso al momento della delibera del documento.

**Art. 40) Sicurezza della rete dati**

1. La rete dati deve essere adeguatamente gestita e controllata. I sistemi e le applicazioni utilizzati nella rete dati devono essere mantenuti in sicurezza, incluse le informazioni in transito.

2. Devono essere definite politiche e procedure per la sicurezza della rete dati. Tutte le attività di manutenzione devono essere tracciate e verificate.
3. Gli aggiornamenti di sicurezza, i livelli di servizio ed i requisiti per la gestione dei servizi di rete devono essere identificati e formalizzati in specifici accordi contrattuali ogniqualvolta la gestione dei servizi sia affidata all'esterno.
4. Le prestazioni della rete dati devono essere controllate per verificare la conformità della gestione rispetto ai parametri attesi.
5. Il miglioramento e potenziamento delle procedure operative per la sicurezza delle reti dati richiederà un arco temporale non inferiore ai due anni e mezzo.

**Art. 41) Sicurezza nello scambio di informazioni**

1. Devono essere predisposte opportune procedure e controlli per lo scambio di informazioni e di software, sia all'interno della ASST che all'esterno, al fine di evitarne la perdita, la modifica o l'uso improprio. Tali attività verranno effettuate secondo il contesto organizzativo aziendale.
2. I supporti contenenti le informazioni devono essere protetti da accessi non autorizzati, manomissioni o alterazioni durante il trasporto.
3. Le informazioni critiche per la ASST contenute nei messaggi elettronici devono essere protette dai rischi di frode, accesso non autorizzato, alterazioni o distruzione mediante l'adozione di idonei sistemi di sicurezza.
4. Le informazioni scambiate nelle transazioni elettroniche devono essere protette al fine di prevenire trasmissioni incomplete, reindirizzamenti, accessi non autorizzati, alterazioni, duplicazioni non autorizzate dei messaggi.
5. Devono essere definite ed attuate specifiche procedure di sicurezza per garantire la protezione delle informazioni correlate ai sistemi a supporto dei servizi istituzionali, in funzione della loro classificazione.
6. Deve essere prevista un'idonea procedura contenente le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato del servizio di posta elettronica.
7. Il miglioramento e potenziamento richiederà, per la completa realizzazione di queste attività, un arco temporale non inferiore ai 3 anni (vedasi piano attuativo allegato).

**Art. 42) Monitoraggio**

1. Le informazioni inerenti alle attività effettuate dagli utenti dei sistemi ICT della ASST e più in generale agli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciate (ad esempio tramite file di log), memorizzate e conservate per un periodo di tempo ritenuto idoneo a supportare la risoluzione di problemi inerenti al funzionamento dei sistemi ICT, le future attività di accertamento e la "gestione degli incidenti", nel rispetto della normativa vigente (es. GDPR [R1], Statuto dei lavoratori [R36]).
2. Analogamente, devono essere definite procedure per il monitoraggio e il successivo accertamento del corretto utilizzo degli strumenti di elaborazione delle informazioni, nel rispetto della normativa vigente (es. Statuto dei lavoratori [R36]).
3. Gli strumenti di monitoraggio devono essere protetti contro i rischi di accesso non autorizzato e/o di alterazione.

4. I guasti ed i malfunzionamenti devono essere tracciati ed analizzati e devono essere intraprese opportune azioni correttive, nel rispetto dei livelli di servizio definiti contrattualmente o in assenza di questi, nel minore tempo possibile per non arrecare degradi prestazionali o rallentamenti delle attività di monitoraggio.

**Art. 43) Crittografia**

1. Ai fini dell'utilizzo della crittografia per la protezione delle informazioni, qualora richiesto, deve essere:
   a) definita una specifica politica di sicurezza;
   b) predisposta ed attuata un'idonea procedura per la gestione delle chiavi crittografiche.
2. Tali politiche e procedure devono risultare conformi alle vigenti normative nazionali ed agli standard internazionali in merito.

**Art. 44) Smaltimento e cancellazione sicura dei dati**

1. Le informazioni trattate presso la ASST devono essere cancellate o distrutte nei casi in cui:
   a) non siano più utili al raggiungimento delle finalità lavorative (ad es. copie di documentazione obsolete o relative a versioni superate o in soprannumero);
   b) siano relative alla cessazione per qualsiasi causa di trattamenti di dati personali/critici non più necessari, pertinenti o eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
   c) gli scopi per le quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi oppure siano diventate incompatibili con tali scopi;
   d) risultino scaduti i termini legittimi di conservazione anche con riferimento al tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati, siano essi determinati da norme di legge generali e/o di settore (ad es. dieci anni per la conservazione delle scritture contabili) oppure dalle finalità per le quali i dati sono stati raccolti o in relazione alle quali devono essere conservati (ad es. contenziosi). La ASST per la conservazione dei dati si attiene ai tempi previsti dal Titolario e Massimario del Sistema Sanitario e Sociosanitario di Regione Lombardia, che deve pertanto essere rispettato;
   e) l'Interessato ne richieda la cancellazione, nell'esercizio dei propri diritti, nei casi applicabili e previsti dalle norme in materia di privacy[R1]. A tal riguardo la ASST ha adottato una specifica procedura per la gestione dei diritti degli interessati, tra cui rientra anche il diritto di cancellazione;
   f) il supporto elettronico sul quale sono memorizzate sia destinato allo smaltimento o dismissione, oppure quando sia destinato al reimpiego da parte di terzi.
2. A tal fine occorre definire un insieme di procedure operative per la cancellazione e distruzione sicura delle informazioni in linea con quanto previsto in materia dal Garante per la protezione dei dati personali [R5][R6]. Tali procedure devono garantire la non recuperabilità delle informazioni e la tecnica di cancellazione deve tenere conto della tipologia di supporto elettronico utilizzato e della classificazione delle informazioni in esso contenute.
3. Deve inoltre essere definito il processo di distruzione sicura di supporti rientranti nella categoria RAEE (Rifiuti e Apparecchiature Elettriche ed Elettroniche), nell'ambito del quale

deve essere garantito il rispetto delle normative ambientali “relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti” e di tutte le altre fonti normative in materia [R1][R35].

# Capo VI - Controllo degli accessi

**Art. 45) Accesso alle informazioni e alle risorse ICT**

1. Deve essere protetto e controllato l'accesso alle informazioni ed alle risorse ICT utilizzate per la loro elaborazione.
2. A tal fine occorre definire formalmente e aggiornare periodicamente una politica di controllo degli accessi sulla base delle esigenze istituzionali della ASST e dei requisiti di sicurezza delle informazioni.
3. Il miglioramento e potenziamento richiederà un arco temporale non inferiore ai 5 anni (vedasi piano attuativo allegato).

**Art. 46) Revisione dei diritti di accesso**

1. Tutti i diritti di accesso assegnati al personale, nonché ai soggetti terzi ai quali l’accesso è consentito per l’esecuzione degli specifici obblighi contrattuali, devono essere regolarmente controllati ed aggiornati.
2. Deve essere prevista la modifica/revoca dei diritti d’accesso quando vengono meno le condizioni per le quali sono stati assegnati (ad esempio a seguito della cessazione del rapporto lavorativo o di cambio della mansione).
3. Si stima l’implementazione delle procedure di miglioramento in un arco temporale non inferiore a 5 anni (vedasi piano attuativo allegato).

# Sezione I - Accessi logici

**Art. 47) Gestione delle credenziali di accesso**

1. Devono essere definiti politiche, procedure ed istruzioni per la gestione delle credenziali di accesso in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali. In tal senso:
   a) il codice identificativo (user-id) deve essere univoco e non riutilizzabile successivamente;
   b) le password devono essere individuali e l’utente è responsabile della loro riservatezza.
2. Inoltre, devono essere definiti standard per la maggiore complessità delle password in proporzione al livello di criticità dell’informazione e al livello di criticità dei sistemi sotto il profilo della sicurezza.
3. Si stima l’implementazione delle procedure di miglioramento in un arco temporale non superiore a 2 anni (vedasi piano attuativo allegato).

**Art. 48) Gestione dei diritti di accesso**

1. Devono essere definiti specifici profili di autorizzazione per l’accesso alle informazioni, da parte degli utenti del sistema informatico della ASST (personale, nonché soggetti terzi ai quali l’accesso è consentito per l’esecuzione degli specifici obblighi contrattuali).

2. I profili di autorizzazione di cui al comma precedente devono consentire di individuare a quali informazioni l'utente può accedere nonché quali azioni può compiere. Al riguardo, le elaborazioni/operazioni autorizzate devono essere limitate a quelle strettamente necessarie allo svolgimento delle mansioni assegnate e nell'ambito di operatività definito, conformemente al principio del "need to know/need to do" e del "at least privilege". In particolare, ai soggetti terzi deve essere consentito l'accesso alle informazioni della ASST solo ed esclusivamente in funzione del proprio incarico.
3. Devono essere definite procedure di gestione e controllo del ciclo di vita dei profili di autorizzazione degli utenti del sistema informatico della ASST (assegnazione, creazione, aggiornamento, disattivazione e revoca), inclusi i profili ad elevati privilegi.
4. Devono essere adottati controlli e procedure di sicurezza in grado di revocare, possibilmente tramite automatismi, i diritti di accesso degli utenti del sistema informatico della ASST.
5. Si stima l'implementazione delle procedure di miglioramento in un arco temporale non superiore a 2 anni (vedasi piano attuativo allegato).

**Art. 49) Responsabilità dell'utente**

1. Devono essere definite idonee istruzioni per rendere edotti gli utenti sulle regole di sicurezza da attuare in merito alla scelta ed all'utilizzo delle password e sulle cautele per assicurarne la segretezza.
2. Tali istruzioni devono, altresì, definire le modalità per il corretto utilizzo delle postazioni di lavoro e degli strumenti informatici e telematici.
3. Il personale e gli eventuali soggetti terzi, ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali, devono essere informati delle conseguenze, disciplinari e anche giuridiche, derivanti dalla mancata applicazione/violazione (volontaria o involontaria) delle istruzioni ricevute.

**Art. 50) Accesso alla rete e relativi servizi**

1. L'accesso alla rete ed ai servizi di rete deve essere consentito solo al personale autorizzato nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
2. In particolare, devono essere:
   a) monitorati gli accessi in conformità alle normative vigenti e regolarmente verificati;
   b) adottati appropriati sistemi di autenticazione per il controllo degli accessi remoti alla rete;
   c) controllati gli accessi fisici e logici per la diagnostica e la configurazione delle porte;
   d) attuati idonei controlli atti ad impedire l'accesso alla rete da parte di utenti non autorizzati.

**Art. 51) Accessi al sistema operativo ed al software di base**

1. L'accesso ai sistemi operativi ed al software di base deve essere controllato da un'idonea procedura di sicurezza.
2. L'accesso al sistema operativo ed al software di base deve essere consentito solo al personale autorizzato nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.

3. Gli accessi devono essere monitorati e periodicamente verificati con cadenza temporale prestabilita, in conformità alle normative vigenti, e regolarmente verificati.
4. Devono essere definite procedure atte ad assicurare la creazione di codici per l'identificazione univoca utenti (user-id).
5. Il sistema deve essere configurato in modo da prevedere la chiusura automatica della sessione lavorativa dopo un periodo predefinito di inattività e la riattivazione della stessa solo previa autenticazione informatica.

**Art. 52) Accessi ai sistemi ed alle applicazioni**

1. L'accesso ai sistemi ed alle applicazioni deve essere controllato da una idonea procedura di sicurezza e limitato al solo personale autorizzato nonché ai soggetti terzi cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
2. Per l'accesso ai sistemi ed alle applicazioni che rivestono particolare criticità è opportuno che l'identificazione avvenga tramite meccanismi di autenticazione forte, la cui robustezza sia proporzionata al livello di criticità dei dati ivi contenuti.
3. Gli accessi ai sistemi ed alle applicazioni devono essere monitorati e regolarmente verificati, nel rispetto della normativa vigente.
4. Devono essere definite idonee procedure e controlli di sicurezza per proteggere i sistemi e le applicazioni dai rischi derivanti dall'utilizzo di computer portatili.
5. Nel caso in cui si utilizzino soluzioni per il lavoro da remoto devono essere definite ed attuate specifiche politiche e procedure per l'accesso in sicurezza ai sistemi ed alle applicazioni.
6. Si stima il miglioramento della gestione e il governo di queste attività in un arco temporale non superiore a 2 anni (vedasi piano attuativo allegato).

# Capo VII - Acquisizione, sviluppo e manutenzione

**Art. 53) Acquisizione, sviluppo e manutenzione dei sistemi**

1. L'acquisizione, lo sviluppo e la manutenzione dei sistemi della ASST deve garantire la protezione delle informazioni da errori, perdite, modifiche non autorizzate o alterazioni.

**Art. 54) Requisiti di sicurezza dei sistemi informativi**

1. La sicurezza deve essere parte integrante dei sistemi informativi utilizzati per la gestione delle informazioni della ASST.
2. L'acquisizione di nuovi sistemi o di parti di sistemi esistenti deve includere, in accordo con i requisiti derivanti dagli scopi istituzionali e dalle politiche di sicurezza, la definizione di specifici requisiti e controlli di sicurezza.
3. Devono essere definiti specifici requisiti per l'identificazione e l'implementazione di appropriati controlli atti ad assicurare l'autenticità e l'integrità dei messaggi tra le applicazioni.

**Art. 55) Sicurezza nei processi di sviluppo e supporto**

1. Le applicazioni, sia commerciali che sviluppate appositamente per la ASST, devono rispettare le politiche e le linee guida di sviluppo sicuro derivanti dagli standard e dalle best practice applicabili.

2. Le applicazioni devono essere protette in modo da impedire errori, perdite, modifiche non autorizzate o alterazioni non autorizzate delle informazioni.
3. Inoltre, qualora possibile, devono essere previsti controlli di congruità delle informazioni, incorporati all'interno delle applicazioni, per rilevare eventuali alterazioni delle medesime derivanti da errori di processo o da azioni deliberate.
4. Per i processi critici devono essere previste procedure per la validazione dei dati inseriti all'interno delle applicazioni al fine di garantire che il dato sia corretto ed appropriato.
5. L'installazione del sistema operativo e dei software di base (middleware, application server, database, ecc.) deve essere controllata e verificata attraverso la predisposizione di idonee procedure di test.
6. Tutte le modifiche apportate ai sistemi devono essere controllate.
7. A seguito delle modifiche al sistema operativo, le applicazioni critiche devono essere controllate e verificate tramite test, al fine di scongiurare eventuali malfunzionamenti dell'operatività e della sicurezza della ASST.
8. Le modifiche ai pacchetti software devono essere limitate allo stretto necessario e, qualora effettuate, strettamente controllate.
9. Devono essere definite idonee procedure per il tracciamento delle modifiche e la successiva verifica.
10. Devono essere definite idonee procedure per la protezione degli ambienti utilizzati per lo sviluppo di nuove applicazioni o per le iniziative di integrazione, in termini di protezione delle informazioni, separazione degli ambienti di sviluppo, test, produzione e specifiche politiche di controllo accesso.
11. Per l'esecuzione dei test, non devono essere utilizzati dati personali ai sensi del GDPR [R1] o dati critici per l'ASST. Qualora fosse strettamente necessario utilizzare i suddetti dati, occorre adottare tecniche di mascheramento o soluzioni similari.
12. I risultati del test devono essere controllati e conservati.

**Art. 56) Sicurezza nella manutenzione**

1. Devono essere adottate procedure ed istruzioni operative per la regolamentazione delle attività di manutenzione dei sistemi informativi. Le procedure devono definire:
   a) i criteri e le modalità per l'aggiornamento periodico dei prodotti utilizzati;
   b) la pianificazione e l'attuazione di interventi di manutenzione programmata (dismissione, sostituzione, ecc.);
   c) il collaudo dell'operatività dei sistemi dopo gli interventi di aggiornamento e manutenzione;
   d) l'aggiornamento della configurazione del sistema in funzione delle modifiche apportate all'ambiente.
2. Tutte le attività di manutenzione devono essere tracciate e regolarmente verificate.
3. Si stima l'implementazione delle procedure di miglioramento in un arco temporale non inferiore ai 3 anni (vedasi piano attuativo allegato). Tale attività è in parte già in essere.

# Capo VIII - Gestione degli incidenti rilevanti ai fini della sicurezza

**Art. 57) Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti**

1. Devono essere identificati, classificati e gestiti, in accordo con le normative nazionali ed interne alla ASST, gli incidenti rilevanti ai fini della sicurezza delle informazioni.
2. Devono essere definite procedure per la gestione degli incidenti rilevanti ai fini della sicurezza delle informazioni in conformità alle vigenti normative nazionali e interne alla ASST ed ai Service Level Agreement (SLA) previsti per i servizi erogati.
3. Tali procedure devono descrivere:
   a) le modalità di monitoraggio, rilevamento e classificazione degli eventi di sicurezza, anche in relazione a quanto richiesto dalle normative applicabili in materia;
   b) le modalità di gestione degli eventi rilevati e le procedure di escalation verso i soggetti interni ed esterni alla ASST;
   c) le finalità, le modalità, i criteri di protezione, di utilizzo ed i tempi di conservazione dei log rilevanti ai fini della ricostruzione delle cause di incidente.
4. La pianificazione e la verifica della risposta e del ripristino a seguito di un incidente devono essere condotti anche con i soggetti terzi, in relazione alle attività da questi svolte in forza degli accordi contrattuali.
5. Tutto il personale della ASST e i soggetti terzi devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nelle istruzioni operative di riferimento, che devono essere opportunamente redatte.
6. Tutto il personale della ASST e i soggetti terzi che individuano o abbiano il sospetto riguardante un incidente di sicurezza, devono segnalarlo immediatamente secondo le modalità appositamente stabilite allo scopo.
7. Devono essere previste sanzioni disciplinari in caso di violazione dei vincoli di sicurezza da parte del personale, in accordo con quanto previsto dalle norme contrattuali vigenti.
8. Devono essere, altresì, previste sanzioni in caso di violazione dei vincoli di sicurezza da parte dei soggetti terzi che accedono ed utilizzano le Risorse Informative per l'esecuzione degli specifici obblighi contrattuali.
9. Si stima l'implementazione delle procedure di miglioramento in un arco temporale non inferiore a 4 anni (vedasi piano attuativo allegato).

# Capo IX - Gestione della continuità operativa

**Art. 58) Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa**

1. Deve essere garantita la continuità operativa della ASST, con l'obiettivo di ripristinare una situazione di normalità entro un tempo prestabilito (in funzione dei livelli di servizio attesi), minimizzando gli impatti sui servizi erogati dall'Amministrazione, derivanti dall'interruzione delle attività a fronte di un incidente di sicurezza, un guasto o disastro.
2. Devono essere identificati e resi noti i requisiti di resilienza a supporto dell'erogazione dei servizi della ASST per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio).
3. Deve essere predisposto un piano di continuità operativa (Business Continuity Plan – BCP), inteso come l'insieme delle attività organizzative e tecnologiche finalizzate alla continuità dei processi che concorrono all'attuazione degli scopi istituzionali della ASST.
4. Tale piano deve descrivere i criteri, le procedure e gli strumenti adottati per la gestione delle emergenze (Contingency Plan) e per il ripristino delle condizioni operative antecedenti al verificarsi di un evento dannoso (Disaster Recovery), in conformità ai livelli di servizio prestabiliti.
5. Il piano deve altresì definire chiaramente la strategia di protezione delle attività istituzionali, sulla base delle attività di analisi e gestione del rischio, rispetto ad eventi di indisponibilità delle informazioni e delle risorse informatiche.
6. La pianificazione e la verifica della risposta e del ripristino a seguito di un evento dannoso che ha impatto sulla continuità operativa della ASST devono essere condotti anche con i soggetti terzi, in relazione alle attività da questi svolte in forza degli accordi contrattuali.
7. Si stima la completa realizzazione di queste attività in un arco temporale di 4 anni (vedasi piano attuativo allegato).

# Titolo VI - Controlli di conformità

**Art. 59) Conformità ai requisiti di sicurezza**

1. La conformità ai requisiti di sicurezza definiti dalle normative cogenti, dagli standard internazionali e dalle best practice applicabili alla ASST, risulta imprescindibile nell'ambito del raggiungimento degli obiettivi di sicurezza espressi dalla Politica della Sicurezza delle Informazioni (cfr. Titolo II - ).
2. Tali requisiti sono presi in considerazione nell'ambito della definizione delle direttive esplicitate negli Statement che indirizzano la tutela delle Risorse Informative della ASST (cfr. Titolo V - ).

# Capo I - Conformità ai requisiti cogenti e contrattuali

**Art. 60) Normativa generale in materia di sicurezza delle informazioni**

1. La ASST deve prevedere un processo di analisi periodica della normativa generale in materia di sicurezza delle informazioni applicabile alla ASST e attuare le attività necessarie per garantire la conformità a tale normativa.
2. In particolare, la ASST, nell'ambito della definizione delle strategie di gestione della sicurezza delle informazioni, deve ottemperare ai requisiti derivanti dai principi generali enunciati dall'attuale legislazione italiana ed europea inerente, a titolo esemplificativo e non esaustivo, alle seguenti tematiche:
   a) Infrastrutture critiche e cybersecurity;
   b) Criminalità informatica;
   c) Tutela del trattamento dei dati personali;
   d) Tutela del software e delle banche dati;
   e) Responsabilità amministrativa e penale a carico di amministratori e dirigenti;
   f) Validità giuridica del documento informatico;
   g) Contratto Collettivo Nazionale di Lavoro e sue integrazioni.

**Art. 61) Normativa specifica e di settore applicabile ai servizi della ASST**

1. La ASST deve prevedere un processo di analisi periodica della normativa specifica e di settore in materia di sicurezza ICT applicabile ai servizi istituzionali erogati dalla ASST e attuare le attività necessarie per garantire la conformità a tale normativa.

**Art. 62) Requisiti contrattuali**

1. La ASST deve documentare e mantenere aggiornati tutti i requisiti contrattuali inerenti alla sicurezza delle informazioni e attuare le attività necessarie per garantire la conformità a tali requisiti.

# Capo II - Conformità a standard internazionali e best practices

**Art. 63) Standard internazionali e best practice**

1. La ASST deve adottare un approccio metodologico, per la gestione delle problematiche inerenti alla sicurezza delle informazioni, conforme agli standard internazionali ed alle best practice nazionali ed internazionali di riferimento per la definizione di ruoli, responsabilità, procedure formali di gestione dei processi legati alla sicurezza, sia per l'operatività della ASST, sia per il trattamento delle emergenze.
2. A tal riguardo occorre prevedere un processo di analisi periodica degli standard internazionali e best practice inerenti alla sicurezza delle informazioni applicabili alla ASST, tra questi identificare quelli più idonei in relazione al contesto della ASST e attuare le attività necessarie per recepirli nel contesto organizzativo.
3. La ASST si impegna alla realizzazione e l'implementazione di tali attività a regime in un arco temporale non inferiore a 3 anni dall'entrata in vigore della presente politica (vedasi piano attuativo allegato).

# Capo III - Riesame della sicurezza delle informazioni

**Art. 64) Verifica e riesame della sicurezza delle informazioni**

1. Devono essere effettuate attività di verifica e riesame, al fine di assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche ed alle procedure della ASST.
2. La ASST deve effettuare, con periodicità predefinita e in occasione di cambiamenti significativi, un riesame indipendente dell'approccio definito per la sicurezza delle informazioni in termini di obiettivi, controlli, politiche, processi e procedure.
3. Deve inoltre essere riesaminata regolarmente la conformità dei processi inerenti alla sicurezza delle informazioni attuati presso la ASST rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza.
4. Infine, devono essere effettuate regolarmente verifiche tecniche dei sistemi informativi al fine di verificarne la conformità rispetto alle politiche e alle norme per la sicurezza delle informazioni.

# Titolo VII - Il sistema documentale

**Art. 65) Sistema documentale per la sicurezza delle informazioni**

1. Il raggiungimento degli obiettivi di protezione delle Risorse Informative della ASST e l'attuazione controlli definiti nel presente documento (cfr. Titolo V - e Titolo VI - ), presuppone la creazione di un adeguato sistema documentale.
2. La ASST ha definito e strutturato il sistema documentale specifico inerente alla sicurezza delle informazioni che consente di indirizzare il governo delle problematiche relative alla protezione delle Risorse Informative. A partire dalla presente politica, tale sistema si sostanzia in Politiche generali e specifiche per la Sicurezza delle Informazioni, Linee Guida, Procedure e Istruzioni operative, secondo il seguente schema:
   a) **Politica per la sicurezza delle Informazioni**: documento (il presente) che fornisce una serie di principi, modalità di azione, requisiti organizzativi, di alto livello e non derogabili, finalizzata a definire l'ambito di applicazione e a guidare il governo della sicurezza delle informazioni, in linea con le volontà dell'Alta Direzione;
   b) **Politiche generali per la Sicurezza delle Informazioni**: documentazione che fornisce regole inderogabili di alto livello su temi generali inerenti alla sicurezza delle informazioni, derivati dalla suddetta Politica per la sicurezza delle Informazioni;
   c) **Politiche Specifiche per la Sicurezza delle Informazioni**: documentazione che fornisce regole inderogabili di alto livello su temi specifici di sicurezza delle informazioni;
   d) **Linee Guida**: documentazione che fornisce raccomandazioni, a carattere generale o specifico, derogabili e la cui implementazione è rimessa alle figure responsabili dei servizi/processi/applicazione. In caso di deroga, le suddette figure devono documentare le ragioni della non aderenza alle linee guida e le scelte effettuate in alternativa;
   e) **Procedure operative**: documentazione che descrive le modalità operative (chi, cosa, come, quando, dove) nell'ambito dei processi di sicurezza e dei controlli implementati per l'attuazione delle Politiche e delle Linee Guida;
   f) **Istruzioni operative**: documentazione descrittiva dei compiti e delle attività effettuate dal personale operativo.
3. Le Politiche, le Linee Guida, le Procedure e le Istruzioni Operative devono essere strutturate in modo semplice e comprensibile al personale di ogni livello organizzativo. Tale documentazione deve essere pubblicata, resa disponibile a tutti i soggetti interessati e revisionata periodicamente.

# Documenti di riferimento

[R1] Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 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 – General Data Protection Regulation (GDPR)

[R2] D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 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 di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[R3] Deliberazione del Garante Privacy numero 53 del 23 novembre 2006: Linee guida in materia di trattamento di dati personali di lavoratori

[R4] Deliberazione del Garante Privacy numero 13 del 1° marzo 2007: Uso delle e-mail e di Internet

[R5] Provvedimento del Garante Privacy del 13 ottobre 2008: Smaltimento e cancellazione sicura dei dati

[R6] Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori - Scheda informativa del Garante per la protezione dei dati personali del 12 dicembre 2008

[R7] Provvedimento del Garante Privacy dell'8 aprile 2010: Videosorveglianza

[R8] Provvedimento del Garante Privacy: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008 e successive modifiche e integrazioni

[R9] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)

[R10] D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Attuazione Direttiva (UE) NIS 2016/1148) aggiornato dal Decreto-Legge 14 giugno 2021, n. 82

[R11] Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019

[R12] Direttiva 2009/136/CE, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e si servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori

[R13] DPCM 29 settembre 2015, n. 178. Regolamento in materia di fascicolo sanitario elettronico

[R14] "Linee guida in materia di Dossier sanitario" del Garante per la protezione dei dati personali del 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015)

[R15] D.lgs. 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

[R16] PIANO NAZIONALE DI RIPRESA E RESILIENZA, #NEXTGENERATIONITALIA, Italia Domani

[R17] DPCM 14 aprile 2021, n. 81. Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del

decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza

[R18] Decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

[R19] D.lgs. 38/2014: Attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, nonché della direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro stato membro

[R20] Framework Nazionale per la Cybersecurity e la Data Protection

[R21] ISO 9001:2008: Sistemi di Gestione per la Qualità - Requisiti

[R22] ISO/IEC 73:2009: Risk management – Vocabulary – Guidelines for use in standards

[R23] UNI ISO 31000: 2010: Gestione del rischio – Principi e linee guida

[R24] ISO/IEC 27001: Tecnologie Informatiche - Tecniche per la Sicurezza - Sistemi di Gestione per la Sicurezza delle Informazioni - Requisiti

[R25] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

[R26] ISO/IEC 27003: Information Technology – Security Techniques – Information security management system implementation guidance

[R27] ISO/IEC 27004: Information Technology – Security Techniques – Information security management - Measurement

[R28] ISO/IEC 27005: Information Technology – Security Techniques – Information security risk management

[R29] D.lgs. n. 82/2005: Codice dell'amministrazione digitale e successive modificazioni e integrazioni

[R30] Misure minime di sicurezza per le PA, AgID

[R31] Determinazione n. 220/2020 del 17 maggio 2020 - Adozione delle Linee Guida – La sicurezza nel procurement ICT, AgID

[R32] Decreto del Direttore Della Repubblica 16 aprile 2013, n. 62: Regolamento recante codice di comportamento dei dipendenti pubblici

[R33] Linee guida regionali per l'adozione dei piani di organizzazione Aziendale delle aziende sanitarie e degli IRCCS di diritto pubblico della Regione Lombardia (DGR n. IX/3822 del 25.07.2012)

[R34] Regolamento (UE) 2019/881 (Cybersecurity act) del 17 aprile 2019

[R35] Decreto Legislativo 3 aprile 2006, n. 152 - Norme in materia ambientale

[R36] LEGGE 20 maggio 1970, n. 300 (Statuto dei lavoratori)

[R37] Regolamento per i procedimenti disciplinari relativi al personale dipendente del comparto della dirigenza della ASST

[R38] Modello Organizzativo Data Protection della ASST

# Allegato 1 – Piano attuativo

**CRONOPROGRAMMA**

| | | 1° ANNO | | | | 2° ANNO | | | | 3° ANNO | | | | 4° ANNO | | | | 5° ANNO | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | TRIMESTRE --> | 1° | 2° | 3° | 4° | 1° | 2° | 3° | 4° | 1° | 2° | 3° | 4° | 1° | 2° | 3° | 4° | 1° | 2° | 3° | 4° |
| **AREA** | **ATTIVITA'** | | | | | | | | | | | | | | | | | | | | |
| **RISCHI LEGATI ALLA CYBERSECURITY** | **Art. 7) Principi generali Adeguatezza al livello di consapevolezza dell'Organizzazione** | | | | | | | | | | | | | | | | | | | | |
| | **Formazione** | | | | | | | | | | | | | | | | | | | | |
| | **Monitoraggio** | | | | | | | | | | | | | | | | | | | | |
| | **Azioni di miglioramento** | | | | | | | | | | | | | | | | | | | | |
| **CONTROLLI DI SICUREZZA** | **Art. 11) Controlli di sicurezza delle informazioni** | | | | | | | | | | | | | | | | | | | | |
| **SICUREZZA DELLE RISORSE INFORMATIVE** | **Art. 13) Inventario degli asset** | | | | | | | | | | | | | | | | | | | | |
| | **Inventario asset informatico** | | | | | | | | | | | | | | | | | | | | |
| | Risorse software, risorse hardware, sistemi informativi esterni e locali | | | | | | | | | | | | | | | | | | | | |
| | Flussi di dati e comunicazioni | | | | | | | | | | | | | | | | | | | | |
| | **Inventario asset cartaceo** | | | | | | | | | | | | | | | | | | | | |
| | **Capitale umano** | | | | | | | | | | | | | | | | | | | | |
| **SICUREZZA NELL'AMBITO DELLE RISORSE UMANE** | **Art. 22) Sensibilizzazione e formazione Sensibilizzazione e formazione del personale ASST e dei collaboratori esterni** | | | | | | | | | | | | | | | | | | | | |
| **SICUREZZA NELLE RELAZIONI CON SOGGETTI TERZI** | **Art. 24) Controlli generali Predisposizione politiche, procedure e istruzioni per gestione e utilizzo delle risorse informative da parte di soggetti terzi** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 25) Clausole Contrattuali** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 26) Monitoraggio, revisione e gestione del cambiamento dei servizi delle terze parti** | | | | | | | | | | | | | | | | | | | | |
| **SICUREZZA FISICA E AMBIENTALE** | **Art. 28) Protezione da minacce di tipo fisico ed ambientale** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 32) Lavorare in aree sensibili Progettazione e implementazione sistemi di sicurezza fisica, definizione procedure per la gestione dell'accesso alle aree sensibili e predisposizione linee guida ed istruzioni per la regolamentazione delle attività all'interno di suddette aree** | | | | | | | | | | | | | | | | | | | | |
| **SICUREZZA DELLE ATTIVITA' OPERATIVE** | **Art. 36) Procedure operative e responsabilità** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 39) Back-up** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 40) Sicurezza delle reti dati - definizione procedure operative** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 41) Sicurezza nello scambio di informazioni** | | | | | | | | | | | | | | | | | | | | |
| **CONTROLLO DEGLI ACCESSI** | **Art. 45) Accesso alle informazioni e alle risorse ICT** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 46) Revisione dei diritti di accesso** | | | | | | | | | | | | | | | | | | | | |
| **ACCESSI LOGICI** | **Art. 47) Gestione delle credenziali di accesso** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 48) Gestione dei diritti di accesso** | | | | | | | | | | | | | | | | | | | | |
| | **Art. 52) Accessi ai sistemi ed alle applicazioni** | | | | | | | | | | | | | | | | | | | | |
| **ACQUISIZIONE, SVILUPPO E MANUTENZIONE** | **Art. 56) Sicurezza nella manutenzione** | | | | | | | | | | | | | | | | | | | | |
| | **Procedure e Istruzioni Operative** | | | | | | | | | | | | | | | | | | | | |
| | **Monitoraggio** | | | | | | | | | | | | | | | | | | | | |
| **GESTIONE DEGLI INCIDENTI RILEVANTI AI FINI DELLA SICUREZZA** | **Art. 57) Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti** | | | | | | | | | | | | | | | | | | | | |
| **GESTIONE DELLA CONTINUITA' OPERATIVA** | **Art. 58) Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa** | | | | | | | | | | | | | | | | | | | | |
| **CONFORMITA' A STANDARD INTERNAZIONALI E BEST PRACTICES** | **Art. 63) Standard internazionali e best practice** | | | | | | | | | | | | | | | | | | | | |