



Proposta	n. PDEL-2025-87 del 09/06/2025
Deliberazione del Direttore Generale	n. DEL-2025-81 del 12/06/2025
Oggetto	Servizio Sistemi informativi e Innovazione digitale. Approvazione della “Policy per la sicurezza delle informazioni” di Arpae Emilia-Romagna.
Dirigente proponente	Servizio Sistemi Informativi e Innovazione Digitale - Cicognani Matteo
Responsabile del procedimento	Cicognani Matteo

Questo giorno *12/06/2025* la sostituta del Direttore Generale, Dott.ssa Manaresi Lia, delibera quanto segue.

VISTI:

- il D.Lgs. 7 marzo 2005, n. 82 “Codice dell’Amministrazione digitale”;
- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, “Regolamento generale sulla protezione dei dati”, conosciuto anche come GDPR;
- il D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (nel seguito anche Codice) come modificato ed integrato dal D.Lgs. 10 marzo 2023, n. 24;
- il “Provvedimento sulle Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema” del Garante per la protezione dei dati personali del 27 novembre 2008, modificato in data 25 giugno 2009;

RICHIAMATA:

- la Deliberazione di Giunta n. 609 del 22/04/2025 con la quale la Regione Emilia-Romagna ha individuato la Dott.ssa Lia Manaresi, Direttore Amministrativo di Arpae Emilia-Romagna, quale soggetto incaricato della sostituzione in via provvisoria del Direttore Generale di Arpae, attribuendole tutti i relativi poteri gestionali, nelle more della nomina del nuovo Direttore Generale dell'Agenzia e comunque non oltre il 15 luglio 2025;

PREMESSO:

- che la tutela del patrimonio delle informazioni riveste importanza strategica per Arpae, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice;
- che il sistema informativo regionale di Arpae è costituito da un’infrastruttura tecnologica molto articolata e complessa, formata da sistemi di elaborazione dati di varia natura, basi dati, apparati di rete e di sicurezza, sistemi software anche complessi;

CONSIDERATO:

- che risulta necessario adottare ogni misura, tecnica ed organizzativa, volta a prevenire il rischio di utilizzo improprio delle strumentazioni informatiche in dotazione e delle banche dati dell’Agenzia, nel rispetto del diritto alla riservatezza e dei diritti dei lavoratori, a promuovere l’utilizzo corretto degli strumenti messi a disposizione per lo svolgimento dell’attività e a verificare l’utilizzo corretto dell’infrastruttura di rete;

CONSIDERATO altresì:

- che la gestione tecnica e la manutenzione degli impianti di elaborazione o di sue componenti comportano in molti casi attività che vanno considerate a tutti gli effetti alla stregua di

trattamenti di dati personali;

RICHIAMATA:

- la D.D.G. n. 62 del 15/05/2025 che individua nella figura del Direttore Generale dell’Agenzia il Titolare del trattamento dei dati personali (ovvero del soggetto a cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso quello della sicurezza) e nella figura dei Responsabili delle strutture i soggetti attuatori degli adempimenti previsti dalla normativa in materia di protezione dei dati personali;

RILEVATO:

- che il Servizio Sistemi informativi e Innovazione digitale di Arpae ha predisposto la “Policy per la sicurezza delle informazioni”, allegata sub A) al presente atto quale parte integrante e sostanziale, contenente le misure tecniche e organizzative adottate da Arpae ai fini di garantire la salvaguardia di riservatezza, integrità e disponibilità delle informazioni agenziali al fine di:
 - definire il sistema documentale del Sistema di Gestione per la Sicurezza Informatica;
 - definire ad alto livello le misure di sicurezza applicate all’interno del Sistema di Gestione per la Sicurezza Informatica;
 - definire ruoli e responsabilità del Sistema di Gestione per la Sicurezza Informatica;

SPECIFICATO:

- che per sicurezza delle informazioni si intende la salvaguardia di riservatezza, integrità e disponibilità delle stesse, in particolare con la “Policy per la sicurezza delle informazioni” suddetta l’Agenzia intende:
 - assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad avervi accesso;
 - salvaguardare l’accuratezza e la completezza delle informazioni e del loro trattamento;
 - assicurare che gli utenti autorizzati abbiano accesso alle informazioni;
- che le misure di sicurezza comprendono:
 - processi di valutazione e gestione costante dei rischi;
 - norme da rispettare per il corretto uso delle strumentazioni informatiche;
 - aggiornamenti costanti del catalogo degli asset;
 - redazione di uno schema di classificazione delle informazioni in termini di riservatezza;
 - integrità, disponibilità e relative regole di sicurezza;
 - controllo degli accessi logici;

- crittografia;
- controllo degli accessi fisici;
- strumenti di gestione dei cambiamenti;
- strumenti di gestione della capacità (risorse utilizzate);
- meccanismi di autenticazione per la sicurezza della rete;
- strumenti di gestione degli incidenti di sicurezza;
- piani di continuità operativa;
- costante monitoraggio, verifiche e controlli di sicurezza;

DATO ATTO:

- che del contenuto della Policy di cui trattasi è stata data informazione al Comitato di Direzione di Arpae nella seduta del 28 maggio 2025;

RITENUTO:

- opportuno approvare la “Policy per la sicurezza delle informazioni”, allegata sub A) al presente atto quale parte integrante e sostanziale, che descrive le misure tecniche e organizzative, ad alto livello, adottate da Arpae ai fini di garantire la salvaguardia di riservatezza, integrità e disponibilità delle informazioni agenziali;
- di disporre la più ampia diffusione della “Policy per la sicurezza delle informazioni” all’interno dell’Agenzia;

SU PROPOSTA:

- del Responsabile Servizio Sistemi informativi e Innovazione digitale, Dott. Matteo Cicognani, che ha espresso il proprio parere sulla regolarità amministrativa del presente atto;

ACQUISITO:

- il parere favorevole del Direttore Tecnico, Dott. Eriberto de’ Munari, ai sensi dell’art. 9 della L.R. n. 44/1995;

DATO ATTO:

- che il responsabile del procedimento è lo stesso Dott. Matteo Cicognani, Responsabile del Servizio Sistemi informativi e Innovazione digitale;

DELIBERA

1. di approvare la “Policy per la sicurezza delle informazioni” di Arpae Emilia-Romagna, allegata sub A) al presente atto quale parte integrante e sostanziale, contenente le regole

tecniche ed organizzative elaborate per garantire la salvaguardia di riservatezza, integrità e disponibilità delle informazioni di Arpa e costituire il fondamento del Sistema di Gestione della Sicurezza delle Informazioni dell'Agenzia;

2. di applicare la suddetta Policy a tutti i soggetti che usufruiscono e gestiscono i servizi del sistema informativo di Arpa;
3. di disporre la più ampia diffusione della "Policy per la sicurezza delle informazioni" all'interno dell'Agenzia.

PARERE: FAVOREVOLE

IL DIRETTORE TECNICO

Firmato digitalmente

Dott. de' Munari Eriberto

LA SOSTITUTA DEL DIRETTORE GENERALE
AI SENSI DELLA D.G.R. N. 609 DEL 22/04/2025

Firmato digitalmente

Dott.ssa Manaresi Lia

Si dichiara che sono parte integrante del presente provvedimento gli allegati riportati a seguire ¹, come file separati dal testo del provvedimento sopra riportato:

¹ L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

arpae emilia-romagna	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 1 di 14

Indice

1. SCOPO	2
2. CAMPO DI APPLICAZIONE	2
3. RIFERIMENTI	2
4. RESPONSABILITÀ	3
5. PROCEDURA	4
5.1. Generalità	4
5.2 Termini e definizione	5
5.3 Il processo di gestione della sicurezza delle informazioni	6
5.4 Il sistema documentale del SGSI	6
5.5 Policy (o politiche) per la sicurezza delle informazioni	6
5.6 Linee guida per la sicurezza delle informazioni	6
5.7 Procedure operative per la sicurezza delle informazioni	7
5.8 Misure di sicurezza del SGSI	7
5.8.1 Gestione del rischio	7
5.8.2 Uso corretto delle strumentazioni informatiche	8
5.8.3 Gestione degli asset	8
5.8.4 Classificazione delle informazioni	8
5.8.5 Controllo degli accessi logici	9
5.8.6 Crittografia	9
5.8.7 Controllo degli accessi fisici	9
5.8.8 Gestione dei cambiamenti	9
5.8.9 Gestione della capacità	9
5.8.10 Sicurezza della rete	10
5.8.11 Gestione degli incidenti di sicurezza	10
5.8.12 Continuità operativa	10
5.8.13 Monitoraggio, verifiche e controlli di sicurezza	10
6 ALLEGATI	11
Allegati 1 : Appendice A – Policy di sicurezza	11
Allegato 2: Appendice B – Linee Guida	12
Allegato 3: Appendice C – Procedure operative	13
7 MODULI	14
8 TABELLA RIASSUNTIVA DELLE REVISIONI	14

Documento firmato digitalmente ai sensi della normativa vigente

Natura modifica: prima emissione		In vigore dal: 12/06/2025
Redazione	Verifica	Approvazione
RSSIID/ M. Cicognani	RSPPE/ S. Ricci	sostituta del Direttore Generale/L.Manaresi

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 2 di 14

1. SCOPO

Il presente documento definisce le misure tecniche e organizzative adottate da Arpae ai fini di garantire la salvaguardia di riservatezza, integrità e disponibilità delle informazioni Agenziali, dato che la tutela di questo patrimonio riveste importanza strategica per l'ente, oltre che essere soggetta a precisi vincoli normativi. Per tale motivo Arpae si è dotata di un Sistema di Gestione per la Sicurezza Informatica (SGSI).

2. CAMPO DI APPLICAZIONE

L'ente, attraverso il SGSI, intende:

- definire un approccio alla sicurezza basato sulla costante valutazione dei rischi;
- definire, implementare e documentare un insieme di misure di sicurezza che permettano di mantenere i rischi ad un livello accettabile;
- adottare un processo di gestione che permetta su base continuativa di garantire che le misure di sicurezza implementate soddisfino le esigenze di sicurezza dell'ente.

Questo documento costituisce “l’Information Security Policy” che si colloca all’interno del sistema documentale del SGSI, con i seguenti obiettivi:

- definire il sistema documentale del SGSI;
- definire ad alto livello le misure di sicurezza applicate all’interno del SGSI;
- definire ruoli e responsabilità del SGSI.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 3 di 14

3. RIFERIMENTI

- ISO/IEC 27001 – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni
- NIST Special Publication 800-53 Security and Privacy Control for Federal Information Systems and Organizations
- COBIT framework – Control Objectives for Information and Related Technologies
- Provvedimento a carattere generale – 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema” e modifiche successive (G.U. n. 300 del 24 dicembre 2008 e G.U. n. 149 del 30 giugno 2009);
- Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati altrimenti detto “General Data Protection Regulation – GDPR”.

4. RESPONSABILITÀ

Responsabilità della Direzione Generale

La Direzione Generale deve garantire il corretto funzionamento del SGSI:

- assicurandosi che sia integrato con tutti i processi aziendali;
- fornendo tutte le risorse necessarie;
- definendo obiettivi di sicurezza delle informazioni, in linea con gli obiettivi strategici aziendali;
- stabilendo la politica per la sicurezza delle informazioni.

Responsabilità dei responsabili dei Servizi di Arpae

Ogni Servizio ha la responsabilità, durante la fase di valutazione dei rischi, di individuare le informazioni critiche trattate all’interno dei processi gestiti e stabilire gli impatti sul business di eventuali perdite di riservatezza, integrità e disponibilità di tali informazioni.

È inoltre responsabilità dei Servizi segnalare tutte le variazioni all’interno dei processi gestiti che possano comportare variazioni sui rischi che insistono sulle informazioni trattate.

Responsabilità del Responsabile del SSIID (RSSIID)

Oltre a quanto detto per i responsabili dei servizi, spetta inoltre:

- l’analisi costi benefici delle misure di sicurezza individuate;
- lo stanziamento del budget necessario per l’applicazione delle misure di sicurezza per le quali l’analisi costi benefici ha dato esito positivo nei limiti del budget assegnato al SSIID;
- la responsabilità della continuità operativa dei sistemi IT aziendali.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 4 di 14

Dal momento che Arpae non dispone di un CISO (Chief Information Security Officer) formalmente nominato, sono in capo al responsabile del SSIIID:

- la definizione delle policy e delle linee guida di sicurezza;
- l'analisi del contesto, la valutazione e il trattamento dei rischi per la sicurezza delle informazioni;
- l'individuazione, la pianificazione, la progettazione e l'implementazione delle misure di sicurezza;
- il monitoraggio della sicurezza, le verifiche e i controlli;
- la gestione degli incidenti di sicurezza;
- in collaborazione con il Servizio Risorse Umane e il Servizio Pianificazione, Progetti Europei, Qualità, Ecomanagement e Formazione, la sensibilizzazione e la formazione degli utenti sui temi della sicurezza delle informazioni.

Responsabilità degli amministratori di sistema

Gli amministratori di sistema, in quanto gestori dei sistemi con i quali vengono trattate le informazioni, ricoprono un ruolo critico all'interno del SGSI. Ricadono pertanto sotto la loro responsabilità:

- la stesura delle procedure operative di sicurezza per i sistemi gestiti;
- l'applicazione delle misure di sicurezza individuate dal RSSIID;
- la partecipazione a tutte le fasi di gestione degli incidenti di sicurezza.

Responsabilità degli utenti

Gli utenti sono responsabili dell'uso delle risorse aziendali a loro assegnate e della tutela delle stesse in termini di disponibilità, integrità e riservatezza, aderendo alla politica aziendale. Sono inoltre tenuti a segnalare sempre eventuali anomalie che possano indicare incidenti di sicurezza.

5. PROCEDURA

5.1. Generalità

Per Arpae, la tutela e la sicurezza del patrimonio delle informazioni riveste un'importanza strategica oltre ad essere soggetta a precisi vincoli normativi.

La sicurezza delle informazioni è definita come la salvaguardia di riservatezza, integrità e disponibilità delle stesse. In particolare:

- tutelare la riservatezza significa assicurare che le informazioni siano accessibili solo a coloro che sono autorizzati ad avervi accesso;

arpae emilia-romagna	POLICY	POL_IS_00
<i>Policy per la sicurezza delle informazioni</i>		Rev.0 del 28/05/25 pag. 5 di 14

- tutelare l'integrità significa salvaguardare l'accuratezza e la completezza delle informazioni e del loro trattamento;
- tutelare la disponibilità significa assicurare che gli utenti autorizzati abbiano accesso, quando richiesto, alle informazioni e agli strumenti ad esse associati.

Per meglio tutelare il proprio patrimonio informativo l'Agenzia adotta un Sistema di Gestione per la Sicurezza Informatica (SGSI). Attraverso il SGSI si intende:

- definire un approccio alla sicurezza basato sulla costante valutazione dei rischi;
- definire, implementare e documentare un insieme di misure di sicurezza che permettano di mantenere i rischi ad un livello accettabile;
- adottare un processo di gestione che permetta su base continuativa di garantire che le misure di sicurezza implementate soddisfino le esigenze di sicurezza dell'ente.

5.2 Termini e definizione

Dir. Gen	Direzione Generale
CISO	Chief Information Security Officer. Il ruolo è svolto, di fatto, attualmente, dal Dirigente responsabile del Servizio Sistemi Informativi e Innovazione Digitale.
Utente	Persona fisica che utilizza gli strumenti elettronici
SSIID	Servizio Sistemi Informativi e Innovazione Digitale.
Servizi Informatici	Sono i servizi messi a disposizione da Arpae per lo svolgimento dell'attività lavorativa in favore degli Utenti per soddisfare un fabbisogno IT. Ad esempio costituiscono Servizi Informatici: Account personale, servizio posta elettronica, Servizio Internet, Servizi applicativi, etc.
Servizi	Unità organizzative dell'ente che svolgono un ruolo specifico all'interno dell'Agenzia
Amministratore di sistema	Chi gestisce e garantisce il corretto funzionamento dei sistemi hardware e software utilizzati per erogare i servizi informatici.
Amministratori di sistema applicativi	Personale non IT che gestisce e garantisce il corretto funzionamento delle applicazioni software complesse utilizzate per erogare servizi interni ed esterni
Tabella RACI	Matrice che assegna le responsabilità specifiche (Responsible, Accountable, Consulted, Informed) per ogni fase di un processo.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 6 di 14

5.3 Il processo di gestione della sicurezza delle informazioni

L'applicazione ed il mantenimento della sicurezza si attuano attraverso misure tecniche e misure organizzative che devono essere parte integrante dei processi di lavoro.

La costruzione di un adeguato processo di gestione della sicurezza delle informazioni comprende le seguenti fasi distinte:

- **pianificazione:** definizione degli obiettivi di sicurezza, analisi dei rischi, individuazione delle misure di sicurezza;
- **implementazione** delle misure di sicurezza: messa in opera di tali misure;
- **controlli:** verifica dell'efficienza e della corretta applicazione delle misure di sicurezza;
- **revisioni:** attuazione di correzioni ed adeguamenti al sistema di protezione delle informazioni sulla base dei risultati ottenuti dai controlli applicati e dagli aggiornamenti normativi e tecnologici.

Tale processo deve essere strutturato su più livelli: a livello strategico, a livello tattico e a livello operativo.

5.4 Il sistema documentale del SGSI

Con sistema documentale del SGSI si intende l'insieme generale dei documenti che descrivono uno o più elementi del SGSI. Tale sistema documentale ha l'obiettivo di definire, diffondere, applicare e far rispettare gli obiettivi di sicurezza dell'Agenzia. Ogni elemento del SGSI viene descritto sotto tutti i possibili punti di vista di interesse e permette di varare e documentare un insieme di misure di sicurezza collocate all'interno di un quadro completo e condiviso a livello aziendale oltre che di definire ruoli e responsabilità di tutti gli attori che partecipano alla gestione della sicurezza delle informazioni.

Poiché ogni singolo aspetto può essere trattato sotto diversi punti di vista, Arpae adotta all'interno del proprio sistema documentale del SGSI diverse tipologie di documenti:

- policy per la sicurezza delle informazioni,
- linee guida per la sicurezza delle informazioni,
- procedure operative per la sicurezza delle informazioni.

5.5 Policy (o politiche) per la sicurezza delle informazioni

Si tratta della tipologia di documentazione di più alto livello nell'ambito del sistema documentale del SGSI, la cui definizione e mantenimento è responsabilità del CISO.

Contiene disposizioni di carattere strategico che non scendono nei dettagli del processo e non definiscono i dettagli implementativi.

5.6 Linee guida per la sicurezza delle informazioni

Si tratta della tipologia di documentazione di livello medio nell'ambito del sistema documentale del SGSI, la cui definizione e mantenimento è ancora responsabilità del CISO.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 7 di 14

Rappresenta un affinamento delle policy di sicurezza, mediante il quale vengono definite le linee guida del processo di attuazione delle misure di sicurezza, definendone il workflow, descrivendone le varie fasi, gli input e gli output, i ruoli e le responsabilità, la tabella RACI.

5.7 Procedure operative per la sicurezza delle informazioni

Si tratta della tipologia di documentazione di più basso livello nell'ambito del sistema documentale del SGSI, la cui definizione e mantenimento è responsabilità degli amministratori di sistema, ognuno per le sue aree di competenza.

Contiene istruzioni passo passo per l'implementazione delle misure di sicurezza richieste dalle policy e definite nei processi.

5.8 Misure di sicurezza del SGSI

Per mantenere i rischi di sicurezza delle informazioni ad un livello accettabile è necessario definire, implementare e documentare un insieme di misure di sicurezza.

In questa policy vengono quindi definite ad alto livello le misure di sicurezza implementate dal SGSI dell'Organizzazione. Ognuna di queste misure è oggetto di documenti specifici, delle diverse tipologie descritte sopra, all'interno del sistema documentale del SGSI.

Le misure di sicurezza comprendono:

- processi di valutazione e gestione costante dei rischi;
- norme da rispettare per il corretto uso delle strumentazioni informatiche;
- aggiornamenti costanti del catalogo degli asset;
- redazione di uno schema di classificazione delle informazioni in termini di riservatezza, integrità, disponibilità e relative regole di sicurezza;
- controllo degli accessi logici;
- crittografia;
- controllo degli accessi fisici;
- strumenti di gestione dei cambiamenti;
- strumenti di gestione della capacità (risorse utilizzate);
- meccanismi di autenticazione per la sicurezza della rete;
- strumenti di gestione degli incidenti di sicurezza
- piani di continuità operativa;
- costante monitoraggio, verifiche e controlli di sicurezza

5.8.1 Gestione del rischio

L'approccio dell'Agenzia alla sicurezza delle informazioni e le misure di sicurezza applicate devono essere basate su un processo di valutazione e gestione costante dei rischi.

A tal fine, almeno annualmente, o in tutti i casi di cambiamenti del contesto, tutti i rischi a cui sono sottoposte le informazioni aziendali devono essere identificati, analizzati e valutati. Eventuali rischi che non possono essere accettati devono essere trattati.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 8 di 14

5.8.2 Uso corretto delle strumentazioni informatiche

Le strumentazioni informatiche che l'Agenzia mette a disposizione devono essere utilizzate da tutti gli utenti Arpae in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale, in modo tale da non compromettere la riservatezza, l'integrità e la disponibilità delle informazioni.

A tal fine, il SSIID, con la collaborazione della Servizio Risorse Umane, ha predisposto apposita documentazione, raccolta organicamente all'interno della "Policy per gli utenti dei sistemi informativi" che contiene norme che tutti gli utenti devono rispettare. Il mancato rispetto o la violazione delle norme è perseguibile con provvedimenti disciplinari previste dal CCNL applicabile all'ente e al regolamento disciplinare aziendale.

Tra gli utenti Arpae rientrano anche gli amministratori di sistema che, in virtù degli ampi privilegi di accesso loro assegnati al fine di poter svolgere la loro attività e della possibilità di accedere direttamente a dati e informazioni critiche senza passare dai meccanismi di controllo accessi e di monitoraggio applicativi, rappresentano un aspetto critico per la sicurezza delle informazioni. Per tali motivi la concessione dei privilegi amministrativi deve essere adeguatamente formalizzata e tracciata, oltre che basata sui principi del minimo privilegio; l'attività stessa degli amministratori di sistema deve essere inoltre tracciata, al fine di poter verificarne il corretto operato.

A tal fine, il SSIID deve predisporre apposita documentazione che disciplini le modalità con cui gli amministratori vengono designati, le modalità con le quali viene mantenuto l'elenco degli amministratori designati e delle loro funzioni, le modalità con le quali viene verificato il loro operato e le norme che tutti gli amministratori di sistema devono rispettare.

5.8.3 Gestione degli asset

Arpae si impegna a gestire un catalogo costantemente aggiornato degli asset rilevanti ai fini della gestione della sicurezza delle informazioni mediante il proprio CMDB (Configuration Management Database); per ciascun asset è individuato un assegnatario che può coincidere con il responsabile della custodia e del corretto utilizzo del medesimo.

5.8.4 Classificazione delle informazioni

Le informazioni critiche per la gestione dei processi aziendali devono essere protette dalla diffusione impropria o da modifiche non autorizzate.

Arpae deve definire uno schema di classificazione delle informazioni in termini di riservatezza, integrità, disponibilità e le relative regole di sicurezza da applicare per la loro protezione in relazione alla classificazione. In assenza di tale schema il SSIID è impossibilitato ad implementare automatismi e politiche generalizzate atte a garantire la protezione di dati e documenti che impediscano la diffusione impropria o le modifiche non autorizzate (al di là dei permessi che i

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 9 di 14

singoli proprietari di file e documenti possono impostare in base alle possibilità di protezione e condivisione forniti dai vari ambienti informatici).

5.8.5 Controllo degli accessi logici

L'accesso ai dati e alle informazioni trattati con strumentazioni informatiche avviene esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.

Ogni utente deve custodire le proprie credenziali di accesso ai sistemi, adottando le necessarie cautele per assicurare la segretezza della componente riservata e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.

Ogni utente deve poter accedere solo all'insieme minimo di risorse necessarie allo svolgimento del proprio lavoro.

Devono essere definite le modalità con cui gli accessi logici vengono concessi, revocati e revisionati e le modalità di autenticazione per l'accesso ai sistemi e alle applicazioni.

5.8.6 Crittografia

Le chiavi crittografiche segrete utilizzate per la cifratura “at rest” e “in motion” delle informazioni devono essere adeguatamente protette e custodite. Gli algoritmi crittografici utilizzati per la cifratura devono consentire un livello di sicurezza adeguato rispetto alla criticità delle informazioni protette.

5.8.7 Controllo degli accessi fisici

L'accesso e la permanenza all'interno delle sedi dell'azienda sono consentiti esclusivamente alle persone autorizzate. Le aree dove sono situati i sistemi e le apparecchiature di elaborazione dei dati sono dotate di un ulteriore meccanismo di controllo accessi basato su badge e monitoraggio accessi basato su sistemi di videosorveglianza.

5.8.8 Gestione dei cambiamenti

I cambiamenti sulle applicazioni e le infrastrutture IT che hanno impatto sulla sicurezza delle informazioni devono seguire un processo ben definito che miri a garantire la sicurezza delle informazioni. La sicurezza delle informazioni deve essere indirizzata in tutte le fasi del processo, a partire dalla fase di progettazione.

5.8.9 Gestione della capacità

Al fine di garantire l'operatività dei servizi e la disponibilità e integrità delle informazioni deve essere implementato un processo di gestione della capacità (utilizzo delle risorse) che indirizzi modifiche all'infrastruttura quando necessario. Il processo deve prevedere il costante monitoraggio dell'utilizzo delle risorse utilizzate per il trattamento delle informazioni, in modo da poter pianificare per tempo le esigenze future in termini di capacità.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 10 di 14

5.8.10 Sicurezza della rete

L'accesso alla rete aziendale deve essere concesso solo agli utenti interni ed esterni autorizzati, mediante dispositivi anch'essi autorizzati. Tale accesso sarà protetto da meccanismi di autenticazione. La rete aziendale deve essere inoltre adeguatamente segmentata in zone contenenti sistemi con livelli di criticità simili o requisiti di sicurezza simili.

5.8.11 Gestione degli incidenti di sicurezza

Gli utenti del sistema IT dell'ente devono operare tempestivamente e in uno spirito di collaborazione per prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile anche al fine di ridurre gli impatti dell'incidente.

Deve essere definito un team dedicato alla gestione degli incidenti di sicurezza, con l'obiettivo di prevenire gli incidenti, di minimizzare gli impatti, di apprendere dagli errori commessi, di comunicare adeguatamente con tutti gli stakeholder.

5.8.12 Continuità operativa

L'ente deve predisporre un piano di continuità operativa e di disaster recovery che permetta di continuare l'erogazione dei servizi IT anche in caso di incidenti gravi o disastri.

Il piano è mantenuto costantemente aggiornato e testato.

5.8.13 Monitoraggio, verifiche e controlli di sicurezza

L'efficienza del SGSI passa anche attraverso un processo di monitoraggio continuo della sicurezza, effettuato a vari livelli e con gradualità.

L'Azienda effettua quindi i controlli ritenuti opportuni per la verifica della corretta applicazione e dell'efficienza delle misure di sicurezza adottate per la protezione delle informazioni e dei dati personali. Tali controlli sono effettuati esclusivamente da personale debitamente autorizzato.

arpae emilia-romagna	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 11 di 14

6 ALLEGATI

Allegati 1 : Appendice A – Policy di sicurezza

Naming convention

Il nome della policy è così costituito:

POL<NN>-<YY><oggetto>-V<XX>

dove:

- **NN**: numero progressivo della policy;
- **YY**: sigla che identifica il tema della policy, per esempio:
 - **SG**: sistema di gestione della sicurezza;
 - **RM**: gestione del rischio;
 - **AS**: asset management;
 - **CL**: classificazione delle informazioni;
 - **AL**: accessi logici;
 - **NS**: sicurezza della rete;
 - **IM**: gestione degli incidenti;
- **oggetto**: oggetto della policy;
- **XX**: numero di versione.

Template

Registro delle modifiche

Si tratta di una tabella nella quale viene tenuta traccia di tutte le modifiche alla policy, con la data della modifica, l'autore, una breve descrizione delle modifiche, la nuova versione della policy.

Data revisione	Versione	Descrizione Modifiche	Autore

Introduzione

Contesto

Questa sezione introduce l'argomento della policy, calandolo nel contesto aziendale.

Scopo e obiettivi

Questa sezione definisce il campo di applicazione della policy in tutte le sue prescrizioni, le distinzioni, e le condizioni di applicabilità. Specifica, inoltre, l'obiettivo o il perché è utile il rispetto della policy.

Revisione e distribuzione della policy

In questa sezione vengono indicati i responsabili della redazione e revisione della policy, i destinatari e le modalità di distribuzione della policy.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 12 di 14

Documenti e normative di riferimento

Questa sezione specifica le leggi, le normative esterne o interne all'ente di riferimento rispetto all'argomento della policy.

Termini e definizioni

Questa sezione specifica i termini che richiedono una definizione precisa, al fine di evitare confusione o ambiguità all'interno della policy. È bene che ad uno stesso termine corrisponda la medesima definizione all'interno di tutto il sistema documentale del SGSI.

Oggetto della policy

Questa sezione costituisce il core della policy, dove viene descritto l'argomento della policy, indicando chiaramente la posizione dell'Azienda sulla questione e i requisiti che devono essere soddisfatti. Sono, inoltre, indicate le eventuali deroghe e le condizioni per la loro concessione. Vengono infine indicati i comportamenti inaccettabili e le conseguenze di tali comportamenti. Le sanzioni possono essere esplicitamente indicate.

Ruoli e responsabilità

Questa sezione viene utilizzata per elencare i ruoli coinvolti nell'implementazione nel rispetto della policy e le loro responsabilità.

Allegato 2: Appendice B – Linee Guida

Naming convention

Il nome della linea guida è così costituito:

LG<NN>-<YY>-<oggetto>-V<XX>

dove:

- **NN**: numero progressivo della linea guida;
- **YY**: sigla che identifica il tema della policy, per esempio:
 - **SG**: sistema di gestione della sicurezza;
 - **RM**: gestione del rischio;
 - **AS**: asset management;
 - **CL**: classificazione delle informazioni;
 - **AL**: accessi logici;
 - **NS**: sicurezza della rete;
 - **IM**: gestione degli incidenti;
- **oggetto**: oggetto della linea guida;
- **XX**: numero di versione.

Template

Registro delle modifiche

Si tratta di una tabella nella quale viene tenuta traccia di tutte le modifiche al documento, con la data della modifica, l'autore, una breve descrizione delle modifiche, la nuova versione del documento.

	POLICY	POL_IS_00
Policy per la sicurezza delle informazioni		Rev.0 del 28/05/25 pag. 13 di 14

Introduzione

Scopo e obiettivi

Vale quanto detto a proposito dell'analoga sezione delle policy.

Revisione e distribuzione

Vale quanto detto a proposito dell'analoga sezione delle policy.

Documenti e normative di riferimento

Vale quanto detto a proposito dell'analoga sezione delle policy.

Termini e definizioni

Vale quanto detto a proposito dell'analoga sezione delle policy.

Ruoli e responsabilità

Questa sezione contiene la tabella RACI, nella quale vengono indicati, per ogni fase del processo, il responsabile dell'attività (Responsible, R), il responsabile dei risultati dell'attività (Accountable, A), le figure coinvolte nell'attività (Consulted, C) e informate dei risultati raggiunti (Informed, I).

Fasi del processo

Questa sezione contiene la descrizione delle varie fasi del processo e, per ognuna di esse, vengono indicate i responsabili dell'attività, le altre figure coinvolte, l'input e l'output.

Workflow

In questa sezione viene rappresentato graficamente il workflow del processo, con l'indicazione dei vari attori coinvolti nelle varie fasi.

Allegato 3: Appendice C – Procedure operative

Naming convention

Il nome della procedura operativa è così costituito:

PR<NN>->YY-<oggetto>-V<XX>

dove:

- **NN**: numero progressivo della procedura operativa;
- **YY**: sigla che identifica il tema della policy, per esempio:
 - **SG**: sistema di gestione della sicurezza;
 - **RM**: gestione del rischio;
 - **AS**: asset management;
 - **CL**: classificazione delle informazioni;
 - **AL**: accessi logici;
 - **NS**: sicurezza della rete;
 - **IM**: gestione degli incidenti;
- **oggetto**: oggetto della procedura operativa;
- **XX**: numero di versione.

Template

Registro delle modifiche

arpae emilia-romagna	POLICY	POL_IS_00
<i>Policy per la sicurezza delle informazioni</i>		Rev.0 del 28/05/25 pag. 14 di 14

Si tratta di una tabella nella quale viene tenuta traccia di tutte le modifiche al documento, con la data della modifica, l'autore, una breve descrizione delle modifiche, la nuova versione del documento.

Introduzione

Scopo e obiettivi

Vale quanto detto a proposito dell'analoga sezione delle policy.

Revisione e distribuzione

Vale quanto detto a proposito dell'analoga sezione delle policy.

Documenti e normative di riferimento

Vale quanto detto a proposito dell'analoga sezione delle policy.

Termini e definizioni

Vale quanto detto a proposito dell'analoga sezione delle policy.

Descrizione della procedura

Questa sezione è il core della procedura, nella quale viene descritto passo passo l'implementazione delle misure di sicurezza.

7 MODULI

Nessuno

8 TABELLA RIASSUNTIVA DELLE REVISIONI

Nella tabella seguente sono riportate le revisioni della presente procedura.

Rev.	del	Natura della modifica	
		Punto	Descrizione
0	28/05/2025	tutti	Prima emissione