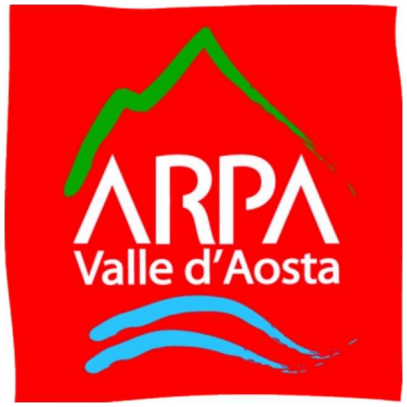

POLITICA DI CIBERSICUREZZA

Cronologia delle modifiche

DATA	Versione	Creato da	Descrizione della modifica
	0.1	IFO A.O. Sistemi informatici e Informativi	Struttura di base del documento

Rif. 0001		POLITICA DI CIBERSICUREZZA		
VERSIONE		**REDAZIONE** IFO A. O. Sistemi informatici e Informativi	**VERIFICA** Direttore Tecnico	**APPROVAZIONE** Direttore Generale
1.0	04/06/2025	Robert Bredy	Marco Cappio Borlino	Igor Rubbo

Sommario

1. Scopo, ambito di applicazione e utenti

Il presente documento definisce l'impostazione strategica adottata dall'**Agenzia Regionale per la Protezione dell'Ambiente** della **Valle d'Aosta** (di seguito anche **ARPA VdA**) per la governance della cibersicurezza: con *Cibersicurezza (o Sicurezza delle Informazioni)* si intende la sicurezza dei dati, con l'obiettivo di garantirne la riservatezza, integrità e disponibilità, degli asset hardware e software ad essa connessi e la tutela della continuità operativa del servizio attraverso l'infrastruttura informatica.

La strategia dell'Agenzia prevede che la politica di cibersicurezza sia organizzata in un sistema organico di Gestione della Sicurezza delle Informazioni **(SGSI)**, su più livelli con struttura ad albero: il più alto è la presente politica che si articola in politiche di secondo livello che, a loro volta, possono prevedere un ulteriore dettaglio più operativo.

Il presente documento, *Politica di cibersicurezza* definisce lo scopo, i principi e le regole di base per la gestione della sicurezza delle informazioni ed è espressione dell'impegno e degli obiettivi della Direzione nella gestione della sicurezza dei dati e della continuità operativa dell'ente nei confronti di minacce informatiche.

Tutte le politiche di secondo livello, le procedure operative e le attività che comportano il trattamento di informazioni o che possono influenzare la sicurezza delle stesse e la continuità del servizio devono essere coerenti con quanto stabilito nella presente politica.

ARPA VdA ha definito una struttura organizzativa adeguata a supportare l'efficace gestione del SGSI. Tale struttura è finalizzata a:

- ridurre al minimo i rischi e garantire la continuità operativa dell'Agenzia limitando in modo proattivo gli impatti delle violazioni della sicurezza.
- assegnare in modo chiaro ruoli e responsabilità per lo sviluppo, l'attuazione e il mantenimento del SGSI;
- garantire l'integrazione del SGSI all'interno di tutti i processi dell'Agenzia, assicurando che eventuali procedure e controlli siano progettati e implementati in modo efficace;
- monitorare costantemente i livelli di esposizione alle minacce che possono compromettere la sicurezza delle informazioni;
- promuovere iniziative di sensibilizzazione e formazione per diffondere una cultura della Sicurezza delle Informazioni a tutti i livelli dell'organizzazione;
- assicurare che le esigenze e le aspettative degli utenti siano soddisfatte in termini di qualità e sicurezza delle informazioni;
- favorire il miglioramento continuo del SGSI stesso attraverso attività di revisione, aggiornamento e ottimizzazione dei processi.

I fruitori di questo documento e dell'intero SGSI sono tutti i dipendenti dell' **Agenzia Regionale per la Protezione dell'Ambiente Valle d'Aosta,** nonché le parti esterne pertinenti.

2. Norme e Standard

Si riporta il contesto normativo nel cui ambito si inserisce il presente documento.

- Legge di “Istituzione del Sistema nazionale a rete per la protezione dell'ambiente e disciplina dell'Istituto superiore per la protezione e la ricerca ambientale” del 28/06/2016, n. 132;
- Nuova disciplina dell’ARPA della Valle d’Aosta (legge regionale 29 marzo 2018, n. 7
- Legge n.90/2024, “Disposizioni in materia di rafforzamento della cibersicurezza nazionale e di reati informatici”.
- D.lgs. 196/2003 Decreto legislativo in merito alla privacy e alla tutela dei dati personali;
- Regolamento (Ue) 2016/679 - Arricchito con riferimenti ai Considerando e aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018

3. Contesto organizzativo dell'Agenzia

Il contesto organizzativo e pianificatorio all'interno del quale si inquadra la Politica per la cibersicurezza è descritto nei seguenti documenti:

- Piano Integrato di Attività e Organizzazione (PIAO);
- Regolamento di funzionamento, Organigramma e Funzionigramma;
- Piano triennale per l'informatica dell'ARPA VdA – 2024-2026 – aggiornamento 2025;
- Codice di comportamento – aggiornamento 2025.

4. Terminologia di base sulla sicurezza delle informazioni

TERMINI	DEFINIZIONI
Riservatezza	Caratteristica delle informazioni in base alle quali sono disponibili solo a persone o sistemi autorizzati.
Integrità	Caratteristica delle informazioni in base alle quali vengono modificate solo da persone o sistemi autorizzati in modo consentito.
Disponibilità	Caratteristica delle informazioni grazie alle quali le persone autorizzate possono accedervi.
Sicurezza delle informazioni	Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni. Si sottolinea che la sicurezza delle informazioni è strettamente connessa con la sicurezza dei sistemi hardware e software e con la continuità su servizio dell'ente.
Sistema di gestione della sicurezza delle informazioni (SGSI)	Parte dei processi di gestione complessivi che si occupa della pianificazione, implementazione, manutenzione, revisione e miglioramento della sicurezza delle informazioni.
ISO/IEC 27001	Norma internazionale che definisce i requisiti per l'impostazione di un SGSI
NDA	Non Disclosure Agreement, accordo di riservatezza

5. Definizione di Ruoli e Responsabilità

RUOLI	RESPONSABILITÀ
Direzione	La Direzione di ARPA VdA è composta dal Direttore Generale, Direttore Amministrativo e Direttore Tecnico i cui ruoli sono descritti nel "Regolamento di Organizzazione".
Direttore generale	Il Direttore generale è responsabile dell'approvazione del presente documento e delle politiche e procedure che ne discendono.
Direttore amministrativo	Il Direttore amministrativo nell'ambito specifico del presente documento ha la responsabilità delle procedure di Acquisto ed è Responsabile della Prevenzione della Corruzione e della Trasparenza.
Direttore tecnico	Il Direttore tecnico predispone e cura gli atti di pianificazione e di programmazione agenziale (DPT e POA) ed ha: • la funzione di Responsabile della transizione digitale • la partecipazione all'attuazione dei sistemi di valutazione, di monitoraggio e di rendicontazione (c.d. ciclo della performance)
Responsabile Transizione Digitale (RTD)	Il Responsabile per la Transizione al Digitale (RTD) è la figura dirigenziale della PA che ha tra le sue principali funzioni quella di garantire operativamente la trasformazione digitale dell'amministrazione.
Referente Cibersicurezza	Il ruolo del Referente della Cibersicurezza ha come scopo principale quello di gestire la strategia di cybersicurezza di un'organizzazione e la sua implementazione per garantire che i sistemi, i servizi e le risorse digitali siano adeguatamente sicuri e protetti. Sulla base dell'articolo 8 della legge n. 90/2024, il referente prevede l'individuazione di una struttura provvede a: a) lo sviluppo delle politiche e delle procedure di sicurezza delle informazioni; b) la produzione e l'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;

	c) la produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) la produzione e l'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) la pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) il monitoraggio e la valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza
Incarico di Funzione Organizzativa A. O. Sistemi informatici e Informativi (IFO - SII).	Figura altamente professionale che ha la responsabilità dell'integrazione dei sistemi di dati, il miglioramento delle reti di comunicazione e il potenziamento della sicurezza delle Informazioni.
Responsabile di Sezione, ufficio o Area operativa	Nell'ambito del presente documento è responsabile della corretta applicazione delle Procedure del SGSI.

6. Obiettivi della Politica di Cibersicurezza e del Sistema di Gestione

ARPA VdA adotta misure di protezione per tutte le informazioni, i beni e le risorse sotto la propria gestione, inclusi quelli ricevuti o forniti da/a soggetti terzi, al fine di salvaguardarne la riservatezza, l'integrità e la disponibilità. Tali misure devono essere proporzionate al valore delle risorse da proteggere e sono applicate nel rispetto delle normative vigenti.

I dati considerati critici sono tutelati contro rischi quali perdita, alterazione, distruzione, accesso non autorizzato o divulgazione indebita. La protezione è garantita attraverso l'impiego di soluzioni tecniche adeguate e procedure operative formalizzate, in linea con i requisiti legali, regolamentari, contrattuali e con le esigenze operative dell'organizzazione.

I sistemi utilizzati per la gestione di informazioni dell'Agenzia sono dislocati in locali sicuri, ad accesso controllato. La protezione è garantita da apposite contromisure per prevenire la violazione della riservatezza e della integrità sia fisica che logica.

È tutelata la Sicurezza delle Informazioni che sono gestite al di fuori dalla sede dell'Agenzia, attraverso specifiche politiche di comportamento comunicate attraverso il documento "Politica sull'utilizzo degli strumenti elettronici e informatici, della posta elettronica e di internet".

Il SGSI prevede obiettivi operativi da definire nel tempo nel quadro di obiettivi strategici di lunga durata propri della Politica di cibersicurezza.

Gli obiettivi del SGSI devono essere pienamente allineati con la strategia, i piani e gli obiettivi complessivi dell'Agenzia.

6.1. Obiettivi strategici

Gli obiettivi strategici prevedono di:

- assicurare la conformità alle normative vigenti e agli obblighi legislativi applicabili;
- implementare iniziative specifiche per rafforzare la governance della cibersicurezza;
- mantenere e introdurre sistemi di protezione del sistema da incidenti di sicurezza (attacchi informatici, fughe di dati, ecc.);
- ridurre i potenziali danni derivanti da incidenti di sicurezza, anche per tutelare l'immagine dell'Agenzia;
- elaborare e aggiornare le politiche, le procedure e le istruzioni operative derivanti dal modello di governance (obiettivi operativi).

6.2. Obiettivi operativi

Gli obiettivi operativi del SGSI sono elaborati annualmente dal Referente Cibersicurezza con il supporto dell'Incaricato di Funzione Organizzativa A.O. Sistemi informatici e proposti al Direttore generale a cui spetta l'approvazione.

Essi sono riportati nell'Allegato A del presente documento che deve essere aggiornato annualmente[1].

Il Referente Cibersicurezza deve rivedere l'SGSI almeno una volta all'anno o ogni volta che si verifica un cambiamento significativo, predisporre la riunione annuale della Direzione ai fini del riesame del sistema e preparare i verbali di tale riunione.

Lo scopo del riesame della Direzione è quello di stabilire l'adeguatezza e l'efficacia del SGSI e l'approvazione dei nuovi obiettivi: particolare attenzione deve essere dedicata alla valutazione degli incidenti informatici che si sono presentati e a quelli mancati (cioè sventati prima che si verificassero).

In sede di riesame del sistema, anche ai fini della definizione di nuovi obiettivi, è necessario considerare almeno i seguenti criteri:

- necessità di adeguare il SGSI all'evoluzione di leggi, regolamenti e norme tecniche;
- necessità di adeguare il SGSI alla pianificazione dell'Agenzia e all'evoluzione tecnologica dei sistemi hardware e software utilizzati;
- variazione di ruoli e responsabilità per attuare al meglio dell'SGSI;
- completezza e adeguatezza delle politiche e procedure operative;
- livello di competenza digitale dei dipendenti;
- livello di adeguatezza delle dotazioni e infrastrutture informatiche.

[1] In sede di prima elaborazione vengono definiti per il biennio 2025-2026

7. Politica

La Politica di Cibersicurezza si articola in un primo livello costituito dal presente documento e da politiche di secondo livello che vengono elaborate come obiettivi operativi del SGSI, vedi par.6.2.

Di seguito sono riportati i principi generali comuni.

7.1. Destinatari

La presente politica si applica a tutte le informazioni, indipendentemente dalla loro natura (cartacea, digitale, verbale, etc.) o forma, nonché a tutti i sistemi utilizzati per la trasmissione, l'elaborazione, la gestione e la conservazione delle stesse. I destinatari della politica sono tutti i dipendenti e i collaboratori dell'Agenzia, incluse le terze parti (come consulenti, studenti e fornitori), che operano all'interno del perimetro organizzativo di ARPA VdA.

Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di ARPA VdA, nonché i visitatori e gli ospiti opportunamente istruiti per il tramite del loro referente in ARPA VdA.

Sono tenuti al rispetto della politica di Sicurezza Cibersicurezza i fornitori di servizi informatici per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni. I fornitori sono tenuti a garantire la protezione delle informazioni riservate e delle proprietà intellettuali loro affidate da ARPA VdA. Devono assicurare la sicurezza, sia fisica sia digitale, delle informazioni trattate, adottando comportamenti improntati alla massima cautela nella gestione di qualsiasi tipologia di dato. È loro responsabilità adottare misure ragionevoli e adeguate a prevenire accessi non autorizzati, perdite o divulgazioni indebite. È fatto espresso divieto di trasmettere informazioni a soggetti terzi senza il preventivo consenso scritto dell'Agenzia.

A tal fine, tutti i contratti stipulati sia con i dipendenti che con fornitori di servizi devono includere specifiche clausole relative alla riservatezza e alla sicurezza delle informazioni (NDA), al fine di formalizzare tali obblighi e garantire la conformità alle politiche di sicurezza di ARPA VdA.

Eventuali esenzioni potranno essere valutate caso per caso dal Referente Cibersicurezza.

7.2. Consapevolezza

La Direzione ARPA VdA promuove azioni per assicurare che ogni dipendente, collaboratore, fornitore o terza parte sia consapevole della presente Politica per la Sicurezza delle Informazioni.

7.2.1. Formazione

Il Referente Cibersicurezza promuove attività di formazione specifica verso la Direzione sulla presente Politica. La Direzione garantisce che ogni risorsa identificata nella presente politica

sia formata alle politiche organizzative applicate e alle procedure relative alla sicurezza delle informazioni.

7.2.2. Divulgazione e comunicazione

L'Agenzia pubblica la Politica per la Cibersicurezza sul proprio sito internet. Inoltre, ARPA VdA attraverso Comunicazioni della Direzione, o altro idoneo strumento, diffonde all'interno dell'ente le disposizioni per la cibersicurezza, così da garantire che tutti i dipendenti di ARPA VdA, nonché le parti esterne coinvolte, siano a conoscenza della presente Politica relativa alla Sicurezza delle Informazioni.

L'area operativa SII, in tale ambito, segnala tempestivamente a tutto il personale, o a chi maggiormente coinvolto, il manifestarsi di potenziali minacce, l'emergere di vulnerabilità, il verificarsi di eventi o incidenti per avviare tempestivamente una risposta adeguata.

7.3. Accettazione della politica di cibersicurezza

Tutti i destinatari sono tenuti a conoscere e accettare formalmente i propri obblighi e le responsabilità individuali in materia di sicurezza delle informazioni.

Tale accettazione è finalizzata a garantire la protezione delle informazioni e dei beni[2] gestiti da ARPA VdA o affidate all'Agenzia da soggetti terzi.

7.4. Responsabilità

Si riportano le responsabilità specifiche per ogni ruolo ricoperto presso l'Agenzia, coerentemente con il Codice di comportamento vigente ed, in particolare con gli articoli 12 (Utilizzo delle tecnologie informatiche) e 18 (Disposizioni particolari per il personale impiegato con la modalità del lavoro agile e altre modalità di lavoro da remoto).

Tutti devono:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di ARPA VdA o affidate ad ARPA VdA da terze parti;
- proteggere i beni materiali, i sistemi informatici e le risorse di ARPA VdA o affidati ad ARPA VdA da terze parti;
- segnalare al personale dell'A.O. SII o al Referente Cibersicurezza il caso di incidenti e/o violazioni della sicurezza effettivi o presunti;
- contattare il personale dell'A.O. SII o il Referente Cibersicurezza, in caso di qualsiasi modifica necessaria della politica di sicurezza, dei requisiti di sicurezza, degli standard, delle procedure informatiche;
- segnalare al personale dell'A.O. SII l'individuazione punti di debolezza del sistema.

[2] Nella misura in cui i beni contengono o danno accesso a dati o garantiscono continuità di servizio

I Dirigenti e gli incaricati di funzione devono:

- verificare il rispetto della politica di sicurezza delle informazioni, delle politiche e delle procedure definite;
- identificare e definire i diritti di accesso delle risorse per le loro attività e responsabilità specifiche;
- definire un livello di rischio accettabile in seguito alla realizzazione di una valutazione dei rischi o della revisione degli stessi;
- richiedere ai fornitori e alle terze parti di rispettare gli accordi di riservatezza e di trattamento dei dati e delle informazioni di ARPA VdA.

Il Referente della cibersicurezza deve:

- determinare il livello di controllo più adeguato da applicare, affinché le misure di sicurezza siano proporzionate al valore delle informazioni e delle risorse da proteggere, nel rispetto delle normative e dei regolamenti vigenti;
- definire i requisiti di sicurezza da considerare nella pianificazione del budget destinato al mantenimento e allo sviluppo dei sistemi informativi dell'Agenzia;
- gestire i principi di governance relativi ai fornitori di soluzioni hardware e software, assicurando la coerenza con la politica di Sicurezza delle Informazioni e promuovendo il miglioramento continuo;
- verificare annualmente lo stato dei sistemi informativi dell'Agenzia, al fine di garantirne la conformità agli standard e alle politiche di sicurezza adottate da ARPA VdA;
- aggiornare l'analisi dei rischi in funzione dell'evoluzione organizzativa, in collaborazione con i dirigenti responsabili;
- garantire la formazione del personale e la crescita della consapevolezza sulle politiche e sulle procedure definite per garantire la Sicurezza delle Informazioni e delle risorse.
- predisporre annualmente o in occasione di cambiamenti significativi riguardanti la cibersicurezza una relazione da presentare in sede di riesame della direzione, contenente le attività svolte e le proposte di miglioramento.

Il personale dell'Area Operativa SII deve:

- implementare la gestione della sicurezza sulla base delle politiche del SGSI;
- verificare il rispetto delle politiche del SGSI;
- gestire i casi di "incidente" in termini di perdita di confidenzialità, integrità e disponibilità delle informazioni, procedendo con la dovuta escalation agli appropriati livelli di Agenzia (i.e. ricevere le segnalazioni, analizzarle, e inoltrarle ai servizi preposti).

L'attuazione di modifiche ai sistemi informatici NON è autorizzata se non pianificata congiuntamente con il Referente Cibersicurezza e l'IFO - SII, concordando tempi e modalità

di implementazione, al fine di garantire la continuità e l'efficacia delle misure di sicurezza in essere.

8. Supporto per l'implementazione dell'SGSI

Con la presente il Referente Cibersicurezza dichiara che il miglioramento continuo dell'SGSI sarà supportato con risorse adeguate, compatibilmente con le risorse di bilancio che l'Agenzia destina alla transizione digitale e con la dotazione organica.

9. Validità

Il presente documento è valido a partire dal 1° luglio 2025.

Allegato A

Per il biennio 2025-26, gli obiettivi operativi previsti consistono nella stesura delle seguenti procedure/politiche.

- Procedura per la gestione e la risposta agli incidenti di sicurezza;
- Procedura per la formazione e l'aggiornamento periodico delle figure apicali;
- Politica di Analisi e valutazione dei Rischi e degli impatti;
- Politica di Gestione degli accessi alle informazioni;
- Politica e Procedura di gestione dei metodi di autenticazione;
- Politica "Bring your own device" (BYOD);
- Politica di responsabilizzazione dei fornitori e delle terze parti.

Sarà inoltre necessario verificare l'aggiornamento dei due seguenti documenti:

- Politica sull'utilizzo degli strumenti elettronici e informatici, della posta elettronica e di internet (Prot. ARPA n 181 del 11/01/2022);
- Istruzione Operativa IO N° 001/SIED Gestione Backup dei server e Ripristino dei dati.