

# Istruzione del Sistema di gestione

## MACROPROCESSO/PROCESSO DI RIFERIMENTO

### Gestione sistemi informativi

# Politica per la Sicurezza delle Informazioni

Sintesi delle modifiche apportate con la presente revisione		
Modifiche ed integrazioni del documento a seguito di indicazioni dell'audit del 10 giugno 2022.		
Par. 1.2 Traduzione in inglese del campo di applicazione		
Par. 1.5 Rivista organizzazione del documento		
Par. 2.9 Dettagliate le relazioni con i fornitori		
Par. 3 Aggiunte responsabilità dirigenti e ufficio ICT		
Par.4 Inserite informazioni di dettaglio relative ai fornitori		
Verificato da	Annamaria Lantero	Resp. SGI
Approvato da	Enrica Bongio	RTD
<i>Pubblicato sul sito Intranet ARPAL a cura dell'Ufficio Sistema di Gestione Integrato</i>		

*Il documento consultabile sul sito Intranet ARPAL è in copia controllata.*



*Il documento in forma cartacea o elettronica archiviata in luogo diverso dal sito Intranet è in copia non controllata, a meno che non riporti la dicitura "COPIA CONTROLLATA N°...." in prima pagina.*

*La diffusione all'esterno di ARPAL del documento deve essere approvata dalla Direzione competente.*

# Politica per la sicurezza delle informazioni

## SOMMARIO

<b>1.</b>	<b><u>SCOPO DEL DOCUMENTO</u></b> .....	<b>3</b>
<b>2.</b>	<b><u>AMBITO DI APPLICAZIONE</u></b> .....	<b>3</b>
<b>3.</b>	<b><u>DEFINIZIONI E ACRONIMI</u></b> .....	<b>4</b>
	3.1 Riferimenti .....	4
	3.2 Organizzazione del documento .....	4
<b>4.</b>	<b><u>POLITICA</u></b> .....	<b>5</b>
	4.1 Accettazione.....	5
	4.2 Accesso.....	5
	4.3 Valutazione .....	5
	4.4 Consapevolezza.....	5
	4.5 Formazione .....	5
	4.6 Rispetto delle leggi e regolamenti obbligatori.....	5
	4.7 Protezione .....	6
	4.8 Sicurezza nella progettazione e sviluppo di soluzioni IT.....	6
	4.9 Relazioni con i fornitori.....	6
<b>5.</b>	<b><u>RESPONSABILITÀ</u></b> .....	<b>7</b>
<b>6.</b>	<b><u>DESTINATARI</u></b> .....	<b>8</b>
<b>7.</b>	<b><u>DIVULGAZIONE E COMUNICAZIONE</u></b> .....	<b>9</b>

	ISTRUZIONE OPERATIVA	
<b>IOP-HWPC-12-AR</b> Ed 1 Rev n°02 del 07/07/22	<h1>Politica per la sicurezza delle informazioni</h1>	Pag 3 di 9

## 1. LA POLITICA PER LA SICUREZZA DELLA INFORMAZIONI

### 1.1 Scopo del documento

Il presente documento riporta la politica aziendale in merito alla gestione delle informazioni, dei dati e degli asset fisici, al fine di garantire la sicurezza delle informazioni e dei dati trattati dall'agenzia, in termini di:

- **Riservatezza:** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- **Integrità:** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- **Disponibilità:** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architettonici associati quando ne fanno richiesta.

La Politica per la Sicurezza definisce le linee guida in base alle quali è stato sviluppato l'intero Sistema per la Gestione della Sicurezza delle Informazioni (SGSI) di ARPAL. Ogni piano e procedura inerente il trattamento delle informazioni o che possa avere impatto con la sicurezza delle informazioni, deve uniformarsi alla politica delineata nel presente documento.

### 1.2 Ambito di applicazione

Campo di applicazione degli interventi è:

*Gestione dei sistemi informativi a supporto dell'erogazione, su rete aziendale ARPAL, dei servizi per gli utenti interni comprensivo delle attività di help desk.*

*Management of information systems to support the provision, on the ARPAL corporate network, of services for internal users including help desk activities.*

La Politica per la Sicurezza delle Informazioni si applica quindi a tutto il patrimonio informativo di ARPAL, costituito dall'insieme delle informazioni residenti nella sede centrale e presso il data center ove sono gestiti i dati aziendali (ad esclusione di quelle in capo e gestite dalla U.O. Clima, Meteo, Idro o da soggetti esterni con servizi di tipo SaS), ed in particolare all'attività di Product Management, ossia alle attività di progettazione e manutenzione di prodotti software e gestione infrastrutture correlate. Tutte le informazioni sopra definite sono accedute in tutte le unità operative dell'agenzia.

Viene definita una struttura organizzativa adeguata a:

- stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del SGSI;
- controllare che il SGSI sia integrato in tutti i processi aziendali e che le procedure e i controlli siano sviluppati efficacemente;
- monitorare l'esposizione alle minacce per la sicurezza delle informazioni;
- attivare programmi per diffondere la consapevolezza e la cultura sulla sicurezza delle informazioni.

Gli obiettivi generali sono quindi:

- garantire i migliori standard, ottimizzando e razionalizzando i processi e gli strumenti aziendali;
- garantire l'efficacia del SGSI;

# Politica per la sicurezza delle informazioni

- garantire la soddisfazione degli utenti in relazione alla qualità e sicurezza delle informazioni.
- garantire il miglioramento continuo

Tutto il personale deve operare per il raggiungimento degli obiettivi di sicurezza nella gestione delle informazioni. L'applicazione del sistema di gestione richiede pertanto piena partecipazione, impegno ed efficace interazione di tutte le risorse umane e tecnologiche.

La continua crescita del livello di servizio verrà perseguita mediante il regolare riesame dello stesso, volto al monitoraggio degli obiettivi prestabiliti e al riconoscimento di eventuali aree di miglioramento. ARPAL è impegnata per:

- 1) attuare, sostenere e verificare periodicamente la presente Politica, a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa;
- 2) garantire le risorse necessarie per l'efficace protezione delle informazioni;
- 3) definire gli obiettivi in materia di sicurezza delle informazioni;
- 4) riesaminare periodicamente gli obiettivi e la Politica per la sicurezza delle informazioni per accertarne la continua idoneità e il miglioramento continuo

Gli obiettivi puntuali verranno poi definiti annualmente nell'ambito del piano triennale di digitalizzazione dell'ente che declinerà puntualmente gli obiettivi per l'anno successivo e per i due anni seguenti a scorrimento.

### 1.3 Definizioni e acronimi

- CCNL Contratto Collettivo Nazionale di Lavoro
- D.lgs. 196/2003 Decreto legislativo in merito alla privacy e alla tutela dei dati personali
- 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)
- ISO/IEC 27001 Norma internazionale che definisce i requisiti per l'impostazione di un SGSI
- NDA Non Disclosure Agreement, accordo di riservatezza
- SGSI Sistema di Gestione della Sicurezza delle Informazioni
- SLA Service Level Agreement, dichiarazione del livello di servizio offerto nell'ambito della fornitura di un servizio

### 1.4 Riferimenti

Nell'ambito del presente progetto sono a disposizione i documenti dell'elenco dei documenti.

### 1.5 Organizzazione del documento

Il documento è articolato su 5 capitoli, compreso il presente che identifica l'ambito di applicazione. Nel Capitolo 2 vengono definiti i principi che costituiscono la Politica per la Sicurezza delle informazioni; nel Capitolo 3 vengono delineate le responsabilità che rientrano nella competenza di diverse figure presenti nell'organizzazione aziendale; nel capitolo 4 vengono identificati i destinatari, anche esterni, ed infine nel capitolo 5 vengono definite le modalità di divulgazione e comunicazione della politica stessa.

# Politica per la sicurezza delle informazioni

## 2. POLITICA

Di seguito sono riportate le policy definite da ARPAL in merito alla sicurezza delle informazioni.

### 2.1 Accettazione

Dipendenti, collaboratori, fornitori, partner, appaltatori e tutte le altre terze parti coinvolti nelle attività istituzionali di ARPAL devono accettare i loro obblighi e le responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse di ARPAL o affidati ad ARPAL da terzi.

Per tale policy si faccia riferimento ai documenti identificati con **L** nell'elenco dei documenti allegato alla presente.

### 2.2 Accesso

Accesso alle informazioni, beni e risorse di ARPAL o affidati ad ARPAL da terzi, devono essere controllati e monitorati sulla base dei seguenti criteri:

- L'accesso è autorizzato solo per le informazioni necessarie (principio della conoscenza minima o need to know);
- L'accesso è autorizzato solo per le informazioni riguardanti specifiche attività.

Per tale policy si faccia riferimento ai documenti identificati con **A** nell'elenco dei documenti allegato alla presente.

### 2.3 Valutazione

ARPAL definisce il giusto rapporto tra:

- le spese necessarie per l'attuazione delle misure al fine di proteggere le informazioni, i beni e le risorse di ARPAL o affidati ad ARPAL da terzi;
- i rischi legati all'utilizzo non autorizzato, modifiche o distruzione.

Per tale policy si faccia riferimento ai documenti identificati con **V** nell'elenco dei documenti allegato alla presente.

### 2.4 Consapevolezza

La Direzione aziendale assicura che ogni dipendente, collaboratore, fornitore o terza parte sia consapevole con la Politica per la Sicurezza di ARPAL e che i suoi comportamenti e gli strumenti utilizzati siano adeguati e in linea con la politica di sicurezza di ARPAL.

Per tale policy si faccia riferimento ai documenti identificati con **C** nell'elenco dei documenti allegato alla presente.



### 2.5 Formazione

La Direzione aziendale garantisce che ogni risorsa sia addestrata sulle politiche organizzative applicate e le procedure relative alla sicurezza delle informazioni.

Per tale policy si faccia riferimento ai documenti identificati con **F** nell'elenco dei documenti allegato alla presente.

### 2.6 Rispetto delle leggi e regolamenti obbligatori

Tutti i trattamenti delle informazioni e le procedure per la sicurezza di ARPAL sono conformi alle leggi e ai regolamenti obbligatori. ARPAL tutela la sicurezza delle informazioni nel pieno rispetto delle leggi e dei regolamenti, anche per quel che riguarda lo specifico riferimento al D.lgs 196/2003 e s.m.i., al regolamento (UE) 2016/679 del Parlamento europeo e del consiglio del 27 aprile 2016

	ISTRUZIONE OPERATIVA	
<b>IOP-HWPC-12-AR</b> Ed 1 Rev n°02 del 07/07/22	<h1>Politica per la sicurezza delle informazioni</h1>	Pag 6 di 9

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) e al CCNL.

Per tale policy si faccia riferimento ai documenti identificati con **N** nell'elenco dei documenti allegato alla presente.

## 2.7 Protezione

Tutte le informazioni, beni e risorse di ARPAL o affidate ad ARPAL da terzi parti sono protette contro i rischi legati al rispetto della riservatezza, dell'integrità e della disponibilità in proporzione al loro valore e in conformità con le leggi vigenti.

Le registrazioni rilevanti sono protette da perdita, distruzione, falsificazione, accessi e divulgazione non autorizzati, in conformità con i requisiti legali, normativi, contrattuali e di business, attraverso appositi strumenti tecnici e procedure operative descritte nei documenti identificati con **P** nell'elenco dei documenti allegato alla presente.

I sistemi che utilizzino canali di comunicazione pubblici (es.: rete Internet) utilizzano il protocollo HTTPS (Hypertext Transfer Protocol Secure) per proteggere l'integrità e la riservatezza dei dati. Le comunicazioni tra sistemi interni sono completamente dentro la LAN aziendale. Entrambe le modalità garantiscono l'autenticità, la riservatezza e l'integrità delle informazioni trasmesse.

I sistemi utilizzati per la gestione di informazioni aziendali 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.

ARPAL, ove possibile, adotta una politica di separazione degli ambienti IT dedicati allo sviluppo, al test/collaudato e all'esercizio dei propri sistemi informativi, al fine di ridurre i rischi di accesso non autorizzato alle informazioni e di modifiche o di indisponibilità dei sistemi di esercizio.

È tutelata la sicurezza delle informazioni che vengono gestite al di fuori del sistema informativo aziendale, attraverso specifiche politiche di comportamento comunicate attraverso il Regolamento Aziendale.

## 2.8 Sicurezza nella progettazione e sviluppo di soluzioni IT

ARPAL adotta un insieme di strumenti descritti nei documenti identificati con **S** nell'elenco dei documenti allegato alla presente, per garantire la sicurezza del processo di sviluppo, al fine di assicurare l'integrità, la disponibilità e la riservatezza dei deliverable realizzati nell'ambito di tale processo.

## 2.9 Relazioni con i fornitori (business partner)

Arpal dispone di istruzioni operative per l'approvvigionamento dei beni e servizi e per il controllo e monitoraggio degli accessi fisici dei fornitori: tutto in una logica di approvvigionamento e di sicurezza fisica.

Il settore Sistemi Informativi, Transizione Digitale e Performance Organizzativa, nella applicazione delle declaratorie funzionali e organizzative di Agenzia, si rapporta con i fornitori HW e SW e adotta la politica di responsabilizzazione dei propri fornitori e delle terze parti con cui collabora per le proprie attività, mediante specifici accordi di riservatezza e sul livello del servizio. Tali accordi sono rivisti con l'emissione di una nuova revisione del modello a valle di ogni revisione della valutazione dei rischi.

# Politica per la sicurezza delle informazioni

ARPAL dispone di una procedura specifica per definire le modalità di gestione delle relazioni con fornitori. Questa procedura riguarda la garanzia del rispetto e della applicazione dei principi di sicurezza di ARPAL. I medesimi possono essere definiti autonomamente nel sistema di gestione delle informazioni del fornitore condivisi e allineati a quelli di Agenzia; a seconda del tipo di fornitura, può comprendere la verifica dei requisiti di sicurezza, fino alla possibilità di eseguire un audit per riscontrare il rispetto di questi requisiti.

Per tale policy si faccia riferimento ai documenti identificati con **B** nell'elenco dei documenti allegato alla presente.

## 3. RESPONSABILITÀ

Le responsabilità di cui al presente capitolo sono generali e riguardano l'intera organizzazione di ARPAL.

Tutti devono:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e delle risorse intellettuali di ARPAL o affidate ad ARPAL da terze parti;
- proteggere i beni materiali, i sistemi informatici e le risorse di ARPAL o affidati ad ARPAL da terze parti;
- proteggere ogni informazione, attività e risorsa sotto la propria responsabilità;
- contattare l'Ufficio preposto o il Responsabile della Transizione al Digitale in caso di violazioni della sicurezza effettive o presunte;
- contattare l'Ufficio preposto o il Responsabile della Transizione al Digitale, in caso di qualsiasi modifica necessaria della politica di sicurezza, dei requisiti di sicurezza, degli standard, delle procedure informatiche.

I Dirigenti Responsabili devono, tra l'altro:

- essere in linea con la politica di sicurezza, i requisiti, gli standard e le procedure definite;
- identificare e definire i diritti di accesso delle risorse per le loro attività e responsabilità specifiche;
- recepire le indicazioni del titolare per il trattamento dei dati per concorrere alla piena applicazione di quanto previsto dalla normativa vigente in tema di privacy e sicurezza delle informazioni;
- 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 essere in linea con gli accordi di riservatezza e di trattamento dei dati e delle informazioni di ARPAL;
- vigilare sull'adempimento di quanto previsto dalla Politica per la sicurezza da parte dei propri dipendenti, dei fornitori e delle terze parti;
- valutare e definire l'accettazione del documento di analisi di rischio

Il Responsabile della Transizione al Digitale deve:

- definire il livello di controllo adeguato da attuare perché i controlli di sicurezza siano proporzionati al valore delle informazioni e delle risorse da proteggere e nel rispetto delle leggi e dei regolamenti obbligatori;

# Politica per la sicurezza delle informazioni

- definire i requisiti di sicurezza di cui è necessario tenere conto nella definizione del budget per il mantenimento e lo sviluppo dei sistemi informativi aziendali;
- gestire i principi di governo dei fornitori HW e SW per quanto concerne la politica di sicurezza delle informazioni e garantire il miglioramento continuo;
- controllare con regolarità lo stato dei sistemi informativi aziendali, per garantire la conformità con gli standard e le politiche di sicurezza di ARPAL;
- svolgere ed aggiornare l'analisi dei rischi nell'evoluzione dell'organizzazione in accordo con i dirigenti responsabili;
- redigere una relazione da presentare in sede di riesame della direzione delle attività svolte e proposte di miglioramento. L'ufficio Performance Organizzativa deve, tra l'altro:
  - fornire gli strumenti utili per monitorare il rispetto delle politiche di sicurezza informatica;
  - fornire gli strumenti utili per monitorare lo stato di avanzamento dello sviluppo e della gestione dei sistemi informativi e dei sistemi di telecomunicazione e fonia in linea alla politica della sicurezza delle informazioni.

L'ufficio ICT deve, tra l'altro:

- garantire e verificare il rispetto delle politiche di sicurezza informatica;

garantire gli strumenti affinché il personale possa formarsi e sia consapevole sulla politica, sui requisiti, sugli standard e sulle procedure definite per garantire la sicurezza delle informazioni e delle risorse. L'ufficio Transizione al Digitale deve, tra l'altro:

- implementare la gestione della sicurezza sulla base delle politiche di sicurezza emesse da ARPAL;
- 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).

Qualsiasi modifica all'organizzazione o ai processi aziendali, alle strutture e ai sistemi di elaborazione delle informazioni che hanno effetto sulla sicurezza delle informazioni, deve essere tempestivamente comunicata al Responsabile della Transizione al Digitale concordando, ove possibile, la tempistica di attuazione.

L'approccio di ARPAL nella gestione della sicurezza delle informazioni e della sua implementazione (obiettivi dei controlli, controlli, politiche, processi e procedure per la sicurezza delle informazioni) viene rivista annualmente nell'ambito dei processi di riesame della Direzione, o in modo indipendente dalla periodicità annuale, quando intervengono cambiamenti significativi.



## 4. DESTINATARI

La politica si applica a tutte le informazioni trattate nell'ambito sopra definito, qualsiasi natura e forma esse abbiano o assumano, e a tutti i sistemi di trasmissione, elaborazione, gestione e memorizzazione utilizzati per il loro trattamento e conservazione nel dominio.

I destinatari della politica sono tutti i collaboratori dell'Agenzia dipendenti o consulenti, a tempo pieno e a tempo determinato. Sono tenuti al rispetto della politica tutti i soggetti che a vario titolo fruiscono dei servizi informativi di ARPAL, nonché i visitatori e gli ospiti opportunamente istruiti per il tramite del loro referente in ARPAL.

Sono tenuti al rispetto della politica di sicurezza delle informazioni i fornitori di servizi informatici per la loro tipica condizione di operare direttamente sui sistemi di gestione delle informazioni. Tutti



	ISTRUZIONE OPERATIVA	
<b>IOP-HWPC-12-AR</b> Ed 1 Rev n°02 del 07/07/22	<h1>Politica per la sicurezza delle informazioni</h1>	Pag 9 di 9

i fornitori sono responsabili della salvaguardia delle informazioni confidenziali e delle proprietà intellettuali, affidate; devono garantire la sicurezza fisica e digitale di tutte le informazioni, devono usare estrema cautela per la protezione di tutti i tipi di informazioni. I fornitori devono adottare provvedimenti ragionevoli atti a garantire la salvaguardia delle informazioni. I fornitori non devono trasmettere informazioni ad altri senza un preventivo consenso scritto.

A tal proposito, nei contratti con tutti fornitori di servizi vengono inserite apposite clausole di riservatezza e di sicurezza delle informazioni.

## 5. DIVULGAZIONE E COMUNICAZIONE

ARPAL pubblica la Politica per la Sicurezza delle Informazioni sul proprio sito internet e sul sito intranet. Inoltre ARPAL attraverso messaggi sulla intranet aziendale nella categoria NewsICT si propone di comunicare estemporaneamente ciò che ritiene importante per la sicurezza delle informazioni e la necessità di conformarsi ai requisiti e alle politiche. In tale ambito affronta problemi di gestione del rischio, obiettivi di sicurezza nuovi o modificati e vulnerabilità, eventi o incidenti per avviare una risposta adeguata a tutti; prevedrà anche messaggi positivi per celebrare i risultati ottenuti e congratularsi con comportamenti di sicurezza corretti.

I messaggi, brevi e focalizzati sul loro vero intento, devono essere chiari nella loro forma e contenuto per produrre il comportamento previsto: si prevede anche di utilizzare piccoli racconti, immagini, metafore o cartoni animati. Nei casi in cui i messaggi debbano essere rivolti a un pubblico specifico, a seconda della classificazione delle informazioni, delle conoscenze tecniche necessarie e del ruolo nell'organizzazione si inviano e-mail differenziate o si pubblicano comunicati chiarendo i destinatari.

L'ufficio preposto mette a disposizione nella intranet aziendale, tramite l'help desk un canale di comunicazione per richieste inerenti la politica di sicurezza delle informazioni, l'organizzazione di sicurezza con i ruoli e le responsabilità chiave, il piano di sensibilizzazione, i requisiti generali e specifici per rispondere agli incidenti, in modo da garantire la comunicazione bidirezionale. L'ufficio preposto ha inoltre schedato a partire dal 2021 un appuntamento con cadenza quindicinale chiamato "ICT Question Time" in cui per 2 ore il personale dell'ufficio è a disposizione in presenza o videoconferenza di tutti gli utenti di ARPAL per ogni domanda inerente l'ICT in ARPAL.

Clausole e requisiti di sicurezza vengono infine inclusi nei contratti per comunicare le esigenze a fornitori di servizi e prodotti.

Allegato 1: Elenco documenti di riferimento