Archiva S.r.l. a socio unico
Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR)
T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com
CF/P.IVA 03237470236 - Capitale sociale: Euro 500.000,00
REA di VR: 319751 Iscritta Registro delle Imprese di Verona

Politica per la sicurezza dei sistemi informativi, delle reti e dei dati

Scopo

La presente Politica definisce il quadro strategico e operativo adottato da Archiva S.r.l. a socio unico, nel seguito anche solo “Archiva” oppure “Organizzazione”, per garantire la sicurezza dei sistemi informativi, delle reti e dei dati in conformità ai requisiti della Direttiva (UE) 2022/2555 (NIS2), così come recepita in Italia con il D.lgs. 7 ottobre 2024, n. 138, del Regolamento di esecuzione (UE) 2024/2690, dello standard ISO/IEC 27001 e della norma EN 17799.

L'obiettivo è stabilire principi, responsabilità e misure di sicurezza volte a:
· proteggere la riservatezza, integrità e disponibilità delle informazioni e dei sistemi informativi;
· assicurare la resilienza operativa delle infrastrutture di rete e dei servizi erogati;
· garantire la conformità normativa in materia di protezione dei dati personali e sicurezza cibernetica;
· prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza informatica;

La presente Politica si applica a:
- tutti i dipendenti, collaboratori, consulenti e fornitori di Archiva, i quali sono tenuti al rispetto vincolante delle disposizioni della presente Politica, delle procedure operative correlate e di ogni altra normativa interna in materia di sicurezza delle informazioni, la cui violazione comporta l'applicazione delle misure disciplinari e contrattuali previste;
- tutti i sistemi informativi, le infrastrutture di rete e i dispositivi tecnologici dell'organizzazione;
- tutti i dati e le informazioni trattate, indipendentemente dal loro formato e dal supporto di memorizzazione su sui vengono tenute;
- tutti i processi aziendali che coinvolgono tecnologie dell'informazione e della comunicazione;
- tutte le sedi operative e i siti remoti dell'organizzazione.

Contesto normativo di riferimento

Ai fini della presente Politica, trovano applicazione le seguenti fonti normative:
- Normativa europea e nazionale
  - Direttiva (UE) 2022/2555 (NIS2) relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, così come recepita in Italia con il D.lgs. 7 ottobre 2024, n. 138
  - Regolamento di esecuzione (UE) 2024/2690 che stabilisce norme tecniche di attuazione per l'applicazione della direttiva NIS2
  - Regolamento (UE) 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
  - Regolamento (UE) 2018/1807 relativo a un quadro per la libera circolazione dei dati non personali nell'Unione europea
- Standard internazionali e norme tecniche
  - ISO/IEC 27001:2022 - Sistemi di gestione per la sicurezza delle informazioni – Requisiti
  - ISO/IEC 27002:2022 - Controlli per la sicurezza delle informazioni

  - ISO/IEC 27017:2015 - Controlli di sicurezza per i servizi cloud
  - ISO/IEC 27018:2019 - Protezione delle informazioni di identificazione personale (PII) nei cloud pubblici
  - ISO/IEC 27701:2019 - Estensione per la gestione della privacy
  - EN 17799:2023 - Requisiti per la protezione dei dati personali nelle operazioni di trattamento
- Normativa e linee guida nazionali
  - D.lgs. 196/2003 (Codice Privacy) e successive modificazioni
  - Linee guida AgID per la formazione, gestione e conservazione dei documenti informatici
  - Framework Nazionale di Cybersecurity e relativi standard ACCREDIA
  - Provvedimenti dell'Autorità Garante per la protezione dei dati personali
- Standard tecnici complementari
  - ETSI EN 319 401 - Politiche generali per i certificati elettronici
  - CEN/TS 18026:2024 - Gestione del rischio nella sicurezza delle informazioni
  - CEN/TS 1870:2025 - Functional requirements for the electronic archiving services

La presente Politica tiene conto dell'evoluzione del panorama normativo e degli standard tecnici, assicurando un aggiornamento continuo per mantenere la conformità e l'efficacia delle misure di sicurezza adottate.

Approccio alla sicurezza

Archiva adotta un approccio sistemico, integrato e proattivo alla sicurezza delle informazioni, alla cybersecurity e alla protezione dei dati, che permea ogni livello dell'organizzazione. Tale approccio si fonda su tre pilastri fondamentali: i) la valutazione e gestione continua dei rischi, ii) il miglioramento costante del sistema di sicurezza, e iii) il coinvolgimento diretto della Direzione, che assume un ruolo guida nella definizione delle priorità e nella supervisione delle iniziative strategiche in ambito sicurezza.

L'adozione di misure tecniche e organizzative è orientata al principio di proporzionalità, ovvero al bilanciamento tra efficacia delle contromisure e impatto sulle operazioni aziendali. Ogni decisione in ambito sicurezza è basata su evidenze oggettive emerse dall'analisi delle minacce e delle vulnerabilità, dall'evoluzione normativa e tecnologica, nonché dal contesto operativo specifico in cui Archiva si trova ad operare.

L'organizzazione riconosce che le minacce alla sicurezza possono avere origine sia interna che esterna, volontaria o accidentale, e pertanto adotta un modello difensivo multilivello che include il monitoraggio continuo degli eventi, l'analisi comportamentale, la gestione tempestiva degli incidenti, la protezione dei dati in tutte le fasi del loro ciclo di vita e il rafforzamento delle capacità di risposta.

L'approccio alla sicurezza non è concepito come un insieme statico di controlli, ma come un ecosistema dinamico e adattivo, in grado di reagire rapidamente ai cambiamenti del contesto e di anticipare le evoluzioni delle minacce. In questo quadro, Archiva considera fondamentale la cultura organizzativa, promuovendo la consapevolezza del rischio tra tutti i livelli aziendali e incentivando comportamenti responsabili e coerenti con gli obiettivi di protezione delle informazioni.

Archiva S.r.l. a socio unico
Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR)
T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com
CF/P.IVA 03237470236 - Capitale sociale: Euro 500.000,00
REA di VR: 319751 Iscritta Registro delle Imprese di Verona

Allineamento strategico

La sicurezza delle informazioni e la cybersecurity costituiscono componenti strutturali della strategia aziendale di Archiva, non semplici requisiti tecnici o tecnologici. Le iniziative in ambito sicurezza sono progettate per sostenere e abilitare gli obiettivi di business, contribuendo in modo determinante alla resilienza dell'organizzazione, alla tutela del valore d'impresa e alla fiducia da parte di clienti, partner e stakeholder istituzionali.
In particolare, la gestione della sicurezza è strettamente integrata con la pianificazione strategica e con i processi decisionali a livello direzionale, in modo da garantire coerenza tra le misure di protezione adottate e le priorità operative, economiche e reputazionali dell'organizzazione. La sicurezza non è considerata un vincolo, ma un elemento abilitante per l'innovazione digitale, la continuità dei servizi e la partecipazione a iniziative pubbliche e private ad alto impatto tecnologico.
L'approccio strategico adottato da Archiva valorizza il ruolo trasversale della sicurezza in tutti i processi aziendali, promuovendo una governance multilivello fondata su responsabilità chiare, processi tracciabili e strumenti misurabili. Le decisioni in materia di sicurezza sono sempre orientate alla sostenibilità, all'efficienza operativa e all'evoluzione futura dell'organizzazione in un contesto normativo e tecnologico in costante cambiamento.

Obiettivi di sicurezza

Gli obiettivi di sicurezza definiti da Archiva rappresentano la cornice di riferimento per tutte le azioni in materia di information security, cybersecurity e protezione dei dati. Essi orientano l'adozione delle misure di sicurezza e costituiscono la base per la valutazione dell'efficacia del sistema di gestione integrato per la sicurezza delle informazioni, la cybersecurity e la data protection.

Nel quadro di riferimento definito, la presente Politica indirizza in via prioritaria i seguenti obiettivi, che rappresentano criteri fondamentali per la misurazione dell'efficacia del sistema di gestione integrato:

1. garantire la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni trattate;
2. prevenire accessi non autorizzati, utilizzi impropri o compromissioni delle risorse informative e tecnologiche;
3. mantenere un adeguato livello di sicurezza fisica, logica, ambientale e delle comunicazioni, in tutte le sedi operative e nei sistemi remoti;
4. supportare la continuità operativa e il ripristino in caso di disastro, minimizzando l'impatto degli eventi critici e assicurando la tempestiva ripresa delle attività;
5. proteggere i dati personali e le informazioni critiche da perdite, alterazioni o trattamenti non autorizzati, in conformità alle normative vigenti e alle buone prassi internazionali.

Il grado di raggiungimento degli obiettivi viene monitorato attraverso indicatori chiave di performance (KPI), rilevati periodicamente e portati a conoscenza della Direzione in occasione dei riesami periodici.

Tali KPI comprendono, a titolo esemplificativo:

1. tassi di conformità ai controlli previsti;
2. numero e tipologia di incidenti segnalati e gestiti;
3. tempo medio di rilevazione e risposta agli eventi;
4. risultati delle attività di audit interni e terze parti;
5. livello di copertura formativa del personale.

I dati raccolti alimentano il ciclo di miglioramento continuo e supportano la definizione di nuove azioni correttive, preventive o di rafforzamento delle capacità di difesa.

Risorse dedicate

Archiva riconosce che l'efficacia del sistema di gestione integrato per la sicurezza delle informazioni, delle reti e dei dati dipende anche dalla disponibilità e adeguatezza delle risorse impiegate. A tal fine, si impegna a garantire la continua allocazione e il rafforzamento delle seguenti risorse:

- Risorse umane: personale con competenze tecniche, organizzative e normative adeguate, supportato da percorsi di formazione e aggiornamento continui, coerenti con i ruoli e le responsabilità assegnate;
- Risorse tecnologiche: infrastrutture, strumenti e tecnologie in grado di supportare l'implementazione e il controllo delle misure di sicurezza, inclusi sistemi di monitoraggio, protezione, risposta agli incidenti e gestione della continuità operativa;
- Risorse metodologiche e organizzative: processi formalizzati, procedure operative, piani di gestione del rischio e strumenti di valutazione dell'efficacia delle misure adottate;
- Risorse finanziarie: budget dedicati alla gestione e al miglioramento delle attività di sicurezza, definiti in modo proporzionale ai rischi individuati, agli obblighi normativi e alle priorità strategiche.

L'adeguatezza delle risorse è oggetto di verifica periodica da parte della Direzione, in occasione dei riesami di cui al paragrafo precedente, e può essere oggetto di adeguamento in funzione dell'evoluzione del contesto operativo, della normativa applicabile e del ciclo di vita dei sistemi.

Ruoli e responsabilità

Archiva ha definito in modo chiaro, formale e documentato i ruoli, le responsabilità e i livelli di autorità in materia di sicurezza delle informazioni, cybersecurity e protezione dei dati. Tali ruoli sono attribuiti in funzione di competenze, autonomia decisionale e collocazione organizzativa, con l'obiettivo di garantire coerenza, accountability e continuità operativa.
In particolare, il Chief Information Security Officer (CISO) — riporta direttamente all'Amministratore Delegato di Archiva ed è coinvolto nella definizione delle priorità strategiche, nella gestione del rischio e nella risposta agli incidenti significativi, come definiti dal decreto NIS[1].

La separazione dei compiti è applicata ove necessario per ridurre conflitti di interesse e garantire un'adeguata segregazione delle funzioni critiche.
I principali ruoli coinvolti sono:

- Organi di amministrazione e organi di direzione: approva la presente Politica, promuove la cultura della sicurezza e garantisce il supporto strategico alle iniziative correlate;
- Chief Information Security Officer (CISO): presidia il sistema di gestione per la sicurezza delle informazioni e coordina le misure di prevenzione, monitoraggio, risposta e miglioramento;
- Chief Technology Officer (CTO): assicura la corretta implementazione tecnica delle misure di sicurezza e la gestione sicura dell'infrastruttura tecnologica;
- Responsabili di Dipartimento: attuano le misure previste nella propria area di competenza e promuovono comportamenti conformi tra i collaboratori;
- Utenti interni ed esterni: operano in conformità alle istruzioni ricevute, partecipano alle attività formative e segnalano eventuali anomalie o violazioni.

L'elenco aggiornato dei ruoli e delle responsabilità è mantenuto nel sistema documentale interno e sottoposto a verifica periodica, anche in funzione di modifiche organizzative o di aggiornamenti normativi.

Comunicazione e consapevolezza

Archiva garantisce che la presente Politica sia comunicata in modo efficace a tutti i livelli dell'organizzazione e condivisa con le parti esterne rilevanti, inclusi fornitori, partner strategici e soggetti terzi coinvolti nei processi aziendali critici.

La Politica è resa accessibile attraverso i canali informativi ufficiali e viene illustrata nei percorsi di onboarding, nei momenti formativi obbligatori e nei programmi di aggiornamento continuo. La sua adozione è vincolante per tutti i soggetti che, a qualunque titolo, accedono ai sistemi informativi e alle infrastrutture digitali di Archiva o trattano dati per conto suo.

Al fine di promuovere una cultura della sicurezza consapevole e diffusa, Archiva attiva iniziative di sensibilizzazione periodica, campagne informative, esercitazioni pratiche e momenti di confronto mirati, anche con il coinvolgimento di figure specialistiche (es. CISO, DPO, CTO, formatori qualificati e altri).
La consapevolezza individuale è considerata un fattore abilitante per la protezione efficace delle informazioni e la prevenzione dei comportamenti a rischio. Per tale ragione, sono previsti strumenti di verifica dell'apprendimento e azioni correttive in caso di comportamenti non conformi o reiterate negligenze.

Archiva S.r.l. a socio unico
Sede legale e operativa: Via Spagna, 24 - 37069 Villafranca di Verona (VR)
T +39 045 2880 000 - sales@archivagroup.it - archivagroup.com
CF/P.IVA 03237470236 - Capitale sociale: Euro 500.000,00
REA di VR: 319751 Iscritta Registro delle Imprese di Verona

Documentazione e conservazione

Archiva mantiene un inventario aggiornato della documentazione rilevante per la sicurezza delle informazioni, delle reti e dei dati, coerentemente con quanto previsto al punto 7.5 delle norme internazionali ISO basate sullo schema HSL definito da ISO. Tale documentazione può comprendere politiche, procedure, linee guida, istruzioni operative, registri, evidenze tecniche e ogni altro artefatto necessario a garantire la tracciabilità, la conformità e l'efficacia del sistema di gestione. Ogni documento è identificato, approvato, diffuso e sottoposto a controllo delle modifiche secondo un ciclo di vita formalizzato, che ne garantisce l'integrità, l'accessibilità e l'allineamento con gli obiettivi aziendali e i requisiti normativi applicabili. La conservazione di tali documenti, qualora richiesta, è disciplinata da criteri basati su obblighi legali, contrattuali, normativi e di auditabilità. I periodi di conservazione sono definiti in apposito documento di "retention" e sono oggetto di revisione periodica, anche in relazione all'evoluzione del quadro regolatorio e dei processi interni. L'accesso alla documentazione è controllato in base al principio del privilegio minimo (least privilege) e può essere oggetto di monitoraggio per garantire la riservatezza e l'integrità delle informazioni gestite. I documenti storici sono archiviati e, ove necessario, resi disponibili per verifiche ispettive o contenziosi.

Politiche specifiche per tematica

La presente Politica rappresenta il punto di riferimento generale per la sicurezza delle informazioni, delle reti e dei dati. Essa è integrata da una serie di politiche tematiche specifiche, che affrontano in modo approfondito aspetti tecnici, organizzativi e procedurali ritenuti critici per la protezione del patrimonio informativo e per l'adempimento degli obblighi normativi.

Tali politiche tematiche sono coerenti con i principi enunciati nel presente documento e sono coordinate all'interno del sistema di gestione integrato di Archiva. Tra le principali politiche tematiche adottate da Archiva rientrano:

- Politica per la gestione dei rischi di sicurezza delle informazioni;
- Politica per il monitoraggio degli eventi di sicurezza;
- Politica per la classificazione e il trattamento delle informazioni;
- Politica per la gestione degli accessi e delle identità digitali;
- Politica per la gestione degli asset e dei dispositivi aziendali;
- Politica per la protezione fisica e ambientale dei sistemi critici;
- Politica per la gestione degli incidenti significativi di sicurezza dei sistemi informativi, delle reti e dei dati;
- Politica per la business continuity e disaster recovery;
- Politica per la sicurezza dei servizi in cloud e dei fornitori esterni;
- Politica per la sicurezza delle comunicazioni e delle reti;
- Politica per la sicurezza delle postazioni di lavoro e dell'endpoint security.

L'elenco completo e aggiornato delle politiche tematiche è conservato nel sistema documentale aziendale e reso disponile, laddove pertinente, sul sito web aziendale, all'indirizzo web X . Ogni politica è approvata formalmente dagli organi di amministrazione e di direzione o, in generale, dagli organi competenti per materia e sottoposta a riesame periodico in coerenza con quanto previsto al paragrafo "Impegno al miglioramento continuo" della presente Politica.

Monitoraggio e indicatori

Archiva definisce un insieme strutturato di indicatori chiave di performance (KPI) e indicatori di maturità per valutare l'efficacia delle misure di sicurezza adottate, il grado di attuazione della presente Politica e il livello complessivo di maturità del sistema di gestione.

In particolare, gli indicatori sono utilizzati per:
- misurare l'efficacia operativa dei controlli e delle procedure implementate;
- valutare il raggiungimento degli obiettivi di sicurezza definiti al paragrafo 5;
- individuare tempestivamente eventuali deviazioni, vulnerabilità o inefficienze;
- orientare le decisioni strategiche in materia di sicurezza informatica;
- supportare le attività di audit, riesame e miglioramento continuo.

Le evidenze raccolte attraverso il monitoraggio sono analizzate con cadenza almeno annuale e presentate alla Direzione. I risultati vengono documentati e, ove necessario, tradotti in azioni correttive, piani di rafforzamento o aggiornamenti delle politiche correlate.
L'organizzazione si riserva di aggiornare gli indicatori nel tempo, per garantirne la coerenza con l'evoluzione del contesto operativo, normativo e tecnologico.

Impegno al miglioramento continuo

Archiva adotta un approccio fondato sul miglioramento continuo, elemento essenziale per garantire l'efficacia, l'adeguatezza e l'evolutività del sistema di gestione integrato per la sicurezza delle informazioni, delle reti e dei dati.

La presente Politica è soggetta a un riesame formale da parte della Direzione almeno una volta all'anno, nonché ogniqualvolta si verifichino:
- cambiamenti significativi nel contesto operativo, tecnologico o normativo;
- mutamenti nella struttura organizzativa o nei processi critici;
- eventi rilevanti, tra cui incidenti significativi, audit esterni o non conformità sistemiche.

Il riesame ha lo scopo di:

- valutare l'effettiva implementazione delle misure previste;
- verificare il livello di raggiungimento degli obiettivi dichiarati;
- recepire i risultati delle attività di monitoraggio e dei feedback provenienti dalle funzioni aziendali coinvolte;
- identificare opportunità di miglioramento e promuovere azioni correttive o preventive.

Tutti i risultati dei riesami sono documentati e resi disponibili per eventuali verifiche, ispezioni o audit da parte di soggetti interni e/o autorità competenti. L'output del processo di riesame contribuisce all'aggiornamento della Politica, delle procedure correlate e degli obiettivi strategici di sicurezza.

Approvazione

La presente Politica è approvata formalmente dagli organi di amministrazione e di direzione di Archiva, che ne garantiscono la legittimazione, la validità e la diffusione a tutti i livelli dell'organizzazione.

La data di approvazione, nonché eventuali modifiche e revisioni successive, sono documentate e tracciate nel sistema di gestione documentale, in modo da garantirne l'integrità, la verificabilità e la disponibilità per le attività di audit o ispezione.