Information Security Policy Document (ISPD)

01.CP_06 - 19/06/2024

Introduzione

Lo scopo della presente politica è quello di definire gli indirizzi strategici adottati da Archiva Group (in seguito anche solo “Archiva”) per salvaguardare la sicurezza delle informazioni, le persone, le società, le organizzazioni e nazioni che in qualsiasi misura interagiscono con Archiva S.r.l. a socio unico, dai rischi di sicurezza della informazioni e dai rischi cyber. Questa politica informa tutti gli stakeholders, interni ed esterni, sui principi guida rilevanti per l’intero ciclo di vista dei dati ai sensi del Regolamento (UE) 2016/679 ed ai sensi del Regolamento (UE) 2018/1807. Archiva considera la protezione del patrimonio informativo un aspetto primario per la salvaguardia e la continuità del proprio business e del business dei propri clienti.

Archiva mira a garantire che:

- le informazioni siano protette dall'accesso non autorizzato o dall'uso improprio;
- la riservatezza delle informazioni sia garantita;
- l'integrità delle informazioni sia mantenuta;
- i concetti di cybersecurity (identify, protect, detect, respond e recover) siano recepiti, implementati e costantemente monitorati e aggiornati;
- la disponibilità delle informazioni e dei sistemi informativi sia mantenuta per l'erogazione dei servizi;
- siano mantenuti i processi di pianificazione e attuazione della continuità operativa;
- siano rispettati i requisiti normativi, contrattuali e legali;
- sia mantenuta la sicurezza fisica, logica, ambientale e delle comunicazioni.

La presente politica è stata approvata dalla Direzione di Archiva e rappresenta l'impegno dell’azienda in materia di Sicurezza delle Informazioni, Cybersecurity oltre che integrare gli obiettivi di business continuity della stessa. La stessa è oggetto di revisione e aggiornamento annuale nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l’idoneità, l’adeguatezza e l’efficacia.

Termini e definizioni

Ai fini del presente documento, si applicano i termini e le definizioni date in:

- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- Regolamento (UE) 2016/679;
- Regolamento (UE) 2018/1807;
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici. (AgID)

Scopo del documento

Il presente documento ha lo scopo di definire la politica per la sicurezza delle informazioni di Archiva, nel suo ruolo di Conservatore, oltre che Intermediario finanziario versi lo SDI e Titolare del trattamento, Responsabile del trattamento (o altro responsabile) ex art. 28 Regolamento (UE) 2016/679.

Archiva ha implementato un Sistema di Gestione Integrato (IMS), comprendente un Sistema di Gestione per la Sicurezza delle Informazioni secondo lo standard tecnico ISO/IEC 27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti), avente come ambito di certificazione la "Progettazione, sviluppo e manutenzione ed erogazione di servizi e prodotti software in modalità SaaS, di fatturazione elettronica, conservazione di documenti informatici, tramite tecniche di firma elettronica, dematerializzazione di archivi cartacei mediante l'applicazione delle Linee guida ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701. Soluzioni di firma elettronica".

Nota 1: ISO/IEC 27017 (Information technology - Security techniques - Code of practice for information security controls based on ISO/IOEC 27002 for cloud services);

Nota 2: ISO/IEC 27018 (Information technology - Security techniques - Code of practices for protection of personally identifiable information (PII) in public cloud acting as PII processors);

Nota 3: ISO/IEC 27701 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

Questo documento è efficace anche per quanto richiesto dal consorzio ENX a proposito della certificazione TISAX.

Archiva persegue quotidianamente il miglioramento continuo del proprio Sistema di Gestione per la Sicurezza delle Informazioni fornendo un fondamentale servizio di supporto al "core business" aziendale attraverso strumenti e mezzi tecnologicamente in linea con il progresso e mantenendoli in perfetto stato di efficienza. L'Azienda definisce i ruoli e le responsabilità del personale coinvolto nella gestione della sicurezza delle informazioni. Identifica periodicamente e sistematicamente le minacce che possono causare danni ai dati, valutandone l'esposizione ai rischi e attuando adeguate azioni di mitigazione.

Archiva forma costantemente il personale coinvolto in qualsiasi trattamento dei dati personali, al fine di proteggere il patrimonio aziendale in conformità alla legge applicabile. Attua, inoltre, programmi di sensibilizzazione, rivolti ai dipendente, ai consulenti esterni, ai partner e agli altri soggetti eventualmente coinvolti in qualsiasi tipo di trattamento, sulla sicurezza delle informazioni e sulla protezione dei dati, con particolare attenzione alla riservatezza, all'integrità e alla disponibilità delle informazioni ed ai dati personali trattati.

Obiettivi

Archiva definendo le linee di indirizzo aziendale riguardanti la protezione dei dati, sulla base della loro classificazione in termini di Riservatezza, Integrità, Disponibilità individua i seguenti obiettivi:

Obiettivi strategici:

- perseguire e mantenere la conformità normativa circa la sicurezza delle informazioni. Archiva S.r.l. persegue la conformità alle leggi e ed ai regolamenti applicabili in ogni contesto operativo e rispetta gli standard tecnici pertinenti all'attività dell'organizzazione.

Obiettivi tattici:

- definire linee di indirizzo generali applicabili in tutti i contesti aziendali, alla sicurezza delle informazioni, qualità, Data Protection e Privacy;

Obiettivi operativi:

- avviare la redazione, la pubblicazione e la periodica revisione di procedure e istruzioni operative necessarie per il conseguimento dei più generali obiettivi tattici e strategici.

Sono stati inoltre definiti e condivisi con gli stakeholder i seguenti documenti di descrizione degli obiettivi:

- Obiettivi per la sicurezza delle informazioni
- Obiettivi per la continuità operativa
- Obiettivi di qualità
- Obiettivi per la prevenzione della corruzione
- Obiettivi per la gestione ambientale

Il presente documento è reso disponibile a tutta l'azienda, attraverso i sistemi informativi adottati, e mantenuto periodicamente aggiornato sulla base dei necessari adeguamenti normativi e tecnologici che tempo per tempo si rendono necessari.

Principi guida

Archiva S.r.l. a socio unico attribuisce primaria importanza alla sicurezza delle informazioni, lavorate per conto dei propri clienti o trattate in prima persona, in considerazione dei crescenti trend di minacce e vulnerabilità, della difficoltà di mantenere nel tempo efficaci misure di sicurezza, ed in fine della cultura aziendale e sensibilità del personale coinvolto nelle operazioni di business.

Per questo motivo sono identificati i seguenti principi elementari:

- la formazione del personale è elemento essenziale per prevenire il manifestarsi di indesiderate situazioni avverse che possono risultare in danno all'azienda ed agli stakeholders coinvolti;
- la formazione specifica nella progettazione di servizi, processi ed applicazioni è elemento indispensabile per garantire l'implementazione di soluzioni che possano corrispondere alle reali necessità dl cliente, nel rispetto delle più accreditate linee guida e prassi di riferimento.
- il continuo monitoraggio di minacce e vulnerabilità è essenziale per garantire la sicurezza ed efficacia dei sistemi e dei servizi erogati ai clienti;
- la continua valutazione delle misure di sicurezza adottate è essenziale per garantire a tuti gli stakeholders il mantenimento dei requisiti minimi di sicurezza delle informazioni.

Ruoli e responsabilità

La matrice sotto riporta i ruoli e le responsabilità assegnate a ciascuna fase del ciclo di vita del presente documento.

Attività	Responsabilità	Esecutore	Consultato	Informato
Redazione, pubblicazione	Direzione aziendale	CISO,CTO	Responsabile di dipartimento , DPO	HR
Adozione	Responsabile di dipartimento	Stakeholder interni e esterni		
Revisione	Direzione aziendale	CISO	Responsabile di dipartimento DPO	HR

Direzione aziendale

La Direzione Aziendale ha la responsabilità complessiva della definizione dei principi generali che regolano la sicurezza delle Informazioni e la loro efficace traduzione in procedure operative interne, necessarie a soddisfare e garantire il corretto funzionamento dei processi operativi stessi oltre che la conformità al quadro normativo di riferimento e i requisiti contrattuali pattuiti.

CISO

Il Chief Information Security Officer è il responsabile della manutenzione del presente documento. La redazione di specifiche ulteriori politiche, procedure ed istruzioni operative è demandata alle singole funzioni aziendali, volta per volta interessate.

Il Chief Information Security Officer (CISO) riporta alla Direzione di Archiva S.r.l. a socio unico ed ha le seguenti responsabilità:

- definire e aggiornare la politica di Sicurezza delle Informazioni sulla base delle linee guida di Sicurezza di Archiva;
- progettare il sistema di protezione e preparare piani per la sua attuazione;
- coordinare l'attuazione del sistema di protezione;
- monitorare l'attuazione dei sistemi di protezione e delle misure di protezione sul patrimonio dei sistemi informativi;
- promuovere iniziative e programmi di formazione, sensibilizzazione e comunicazione in materia di Sicurezza informatica;
- promuovere attività di audit e valutazione per il monitoraggio continuo dell'adeguatezza e dell'efficacia del sistema di protezione delle informazioni;
- riportare alla Direzione di Archiva lo stato del sistema di sicurezza delle informazioni, i piani, le azioni e le problematiche.

Il CISO, è anche Responsabile dell'IMS e, pertanto, è responsabile di:

- progettare l'IMS e preparare piani per la sua attuazione;
- coordinare l'attuazione dell'IMS;
- mantenere e monitorare l'IMS.

CTO

Il Chief Technology Officer (CTO) riporta alla Direzione di Archiva S.r.l a socio unico ed ha le seguenti principali responsabilità:

- definire gli obiettivi e le strategie per il reparto IT;
- selezionare e implementare la tecnologia adatta per semplificare tutte le operazioni interne e contribuire a ottimizzare i loro vantaggi strategici;
- progettare e personalizzare i sistemi e le piattaforme tecnologiche per migliorare la Customer Experience;

Il CTO è anche il Responsabile dell'IMS e, pertanto, è responsabile di:

- pianificare l'implementazione di nuovi sistemi e fornire indicazioni ai professionisti IT e ad altro personale all'interno dell'organizzazione;
- approvare gli acquisti di attrezzature tecnologiche e software e stabilire partnership con fornitori IT;
- supervisionare l'infrastruttura tecnologica nell'organizzazione (reti e sistemi informatici), per garantire prestazioni ottimali;
- dirigere e organizzare progetti legati all'ambito IT;
- monitorare i cambiamenti o i progressi tecnologici per scoprire i modi in cui l'azienda può ottenere un vantaggio competitivo;
- analizzare i costi, il valore e i rischi della tecnologia dei sistemi informatici per consigliare il management e suggerire azioni.

DPO

Il DPO (Responsabile per la protezione dei dati) nell'ambito del presente documento ha il compito di informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono le attività di trattamento circa gli obblighi derivanti dal presente documento, dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Il DPO ha, inoltre, il compito di sorvegliare l'osservanza del presente documento per quanto attiene al trattamento dei dati personali e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Responsabili di Dipartimento

I Responsabili di Dipartimento di Archiva S.r.l a socio unico sono tenuti, secondo le proprie responsabilità, ad applicare e monitorare l'attuazione di tutte le norme in materia di sicurezza delle informazioni e a segnalare alla Direzione Aziendale, al CTO e al CISO qualsiasi questione sullo stato di sicurezza delle informazioni (es.: violazioni dei sistemi, stato di avanzamento del rispetto delle misure di sicurezza, ecc.). Sono, inoltre, tenuti ad informare i fornitori e i consulenti che svolgono attività per conto di Archiva, delle linee guida e delle procedure di protezione necessarie per il trattamento delle informazioni.

I Responsabili devono adoperarsi per garantire la traduzione dei principi definiti attraverso la presente politica all'interno dei propri reparti e dei processi da essi governati.

Utenti interni

Gli utenti interni (dipendenti/collaboratori) trattano le informazioni sulla base di istruzioni e autorizzazioni definite in base a specifici profili operativi. Gli utenti interni sono responsabili per l'adozione di misure comportamentali in linea con i principi definiti all'interno del presente documento di politica e con le Istruzioni Operative per gli Autorizzati al trattamento dei dati redatte ex art. 29 del Regolamento (UE) 2016/679.
Agli utenti interni è richiesta, inoltre, la conoscenza ed il rispetto del Regolamento Aziendale e del Regolamento Informatico Aziendale. Ogni comportamento in violazione di quanto sopra sarà volta per volta valutato dalla Direzione Aziendale, la quale si riserva fin da ora la possibilità di ricorrere ad azioni disciplinari per quanto già previsto dal CCNL di riferimento.

OGNI DIPENDE E COLLABORATORE DI ARCHIVA, AL PARI DI UTENTI ESTERNI AI QUALI PER SPECIFICHE RAGIONI VIENE CONCESSO L'ACCESSO AI SISTEMI INFORMATIVI AZIENDALI, È TENUTO A RISPETTARE LE DISPOSIZIONI DELLA PRESENTE POLICY DI SICUREZZA DELLE INFORMAZIONI.

LA VIOLAZIONE DI QUESTA POLITICA E DEI REQUISITI DI SICUREZZA DA QUESTA DISCENDENTI, POTRÀ RISULTARE IN DANNO ALL'AZIENDA LA QUALE SI RISERVA FIN DA ORA LA FACOLTÀ DI INTRAPRENDERE PROVVEDIMENTI DISCIPLINARI O AZIONI LEGALI NELLE OPPORTUNE SEDI.

Principali risultati attesi

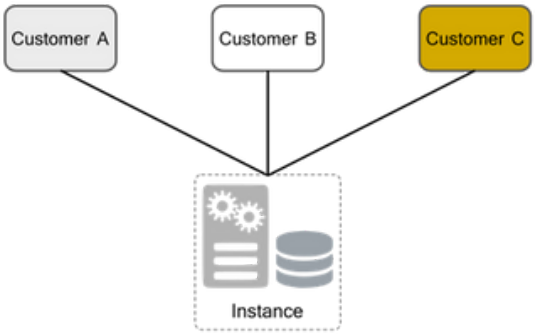
L'introduzione della presente politica pone le base per la definizione di ulteriori politiche, procedure e istruzioni operative le quali sono fin da ora ispirate ed informate dei principi generali qui definiti, con la cui applicazione l'Azienda vuole garantire il raggiungimento degli obiettivi strategici sopra citati.

Relazioni con altre politiche

Alla presente politica è implicitamente collegata ogni altra ulteriore politica implementata da Archiva.

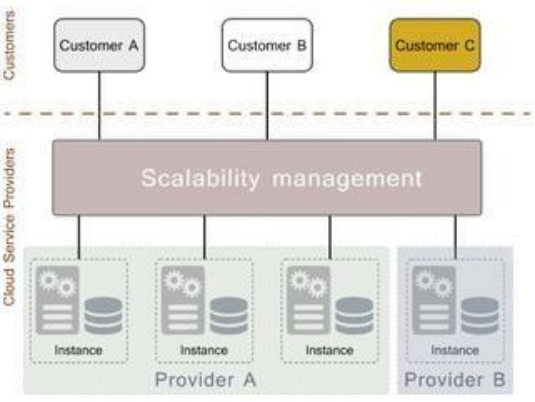
Considerazioni specifiche per l'erogazione di servizi in cloud e per il trattamento di dati personali nel cloud

A partire dal 2019, Archiva ha avviato un percorso di avvicinamento all'erogazione dei servizi resi a clienti, tramite il cloud. Archiva ha ora adottato un modello "Multi-tenant SaaS application", schematizzato nell'illustrazione seguente: (immagine tratta dalla circolare AgID n° 3 del 9 aprile 2018)



Una singola istanza applicativa serve contemporaneamente più clienti, i quali accedono alla medesima istanza applicativa in esecuzione su risorse virtuali condivise. L'isolamento dei dati e degli utenti
avviene a livello applicativo, di gestione delle basi di dati (DBMS) e degli storage, utilizzando gli opportuni meccanismi di autenticazione, autorizzazione e sicurezza

Nel percorso di rinnovamento della propria infrastruttura, orientato al Cloud, il nuovo modello, di seguito illustrato, permetterà di avere configurazioni più flessibili.



I clienti potranno avere la loro istanza applicativa in esecuzione su risorse condivise o dedicate (o un misto delle due) in maniera trasparente e configurabile. Il sistema di load balancing permette di implementare le politiche di allocazione (delle nuove istanze applicative) in funzione di una moltitudine di criteri (uno dei più importanti è la qualità del servizio). Le istanze applicative potranno essere aggiunte e rimosse dinamicamente in qualunque momento ed in base alle esigenze. Anche le risorse virtuali necessarie alle applicazioni sono allocate in modo dinamico. L'allocazione di nuove istanze applicative o di risorse virtuali non richiede nessuna modifica architetturale del sistema che è già stato realizzato in modo da adattarsi dinamicamente. Tutto ciò permette di offrire ed attuare SLA diversificati per i vari clienti.

La baseline di sicurezza di Archiva, si estende, quindi, ai controlli di sicurezza delle linee guida sopra citate, le quali devono, dunque, essere tenute in considerazione per quanto dichiarato nello scope di certificazione, con particolare riferimento alla progettazione ed allo sviluppo di prodotti finalizzati alla realizzazione di servizi che verranno erogati tramite il cloud.

Questa nuova prospettiva richiede, inoltre, che:

- le attività di Risk Assessment tengano maggiormente in considerazione i rischi derivanti da attività seguite da autorizzati all'interno di Archiva;
- sia verificata la segregazione logica e, dove pertinente, fisica degli ambienti applicativi concessi in uso ai clienti;
- sia sempre verificata la possibilità di accesso alle informazioni (asset) dei clienti, ospitate e trattate in ambito cloud;
- sia periodicamente verificata ed aggiornata la procedura di comunicazione verso i clienti, in occasione dell'applicazione di change;
- sia periodicamente verificata la sicurezza degli ambienti virtualizzati su cui si base l'infrastruttura cloud;
- sia periodicamente eseguito un processo di rivalutazione delle utenze concesse in uso ai clienti;
- sia prevista la comunicazione di Data Breach ed il supporto alle attività investigative connesse.

Tutti i servizi erogati in cloud, sono sotto il controllo della struttura “Archiva Information Security" (cfr. HLP_02 Leadership). Al termine della fase di progettazione del servizio, la funzione Project Management comunica alla funzione Customer Care i riferimenti del cliente per le successive ed eventuali attività di assistenza.

Archiva si impegna a osservare, fra le altre, la normativa tempo per tempo vigente in materia di Data Protection & Privacy.

Controlli Crittografici

In considerazione della attività proprie di intermediario verso il SDI e di Conservatore, iscritto al Marketplace AgID Conservatori, da cui discendono i conseguenti vincoli generali, di qualità, di sicurezza e organizzativi, Archiva al fine di proteggere i dati trattati per conto dei propri Clienti quando questi sono a riposo, può adottare meccanismi crittografici, in base a quanto concordato in sede di redazione del progetto.
Archiva si è dotata di una procedura interna “POA.SYS.07 - Utilizzo della crittografia”, contenente ulteriori elementi generali dei sopracitati meccanismi crittografici a protezione del dati in transito.

Gestione del Cambiamento

Tutte le modifiche maggiori apportate ai servizi erogati ai clienti, devono essere preventivamente comunicate indicando la data di applicazione di tali modifiche, la loro descrizione e eventuali impatti sull'operatività dei clienti. Archiva ha implementato un processo di gestione dei cambiamenti, governato dalla procedura interna “POA.CISO.05 - Change management”.

Backup

Archiva implementa diverse soluzioni di backup specifiche per i dati trattati e per gli ambienti server virtuali utilizzati nell'erogazione dei servizi applicativi.

Archiva implementa 2 diversi sistemi di backup:

- Veeam Backup & Replicator per Database, Server ed application server;
- SnapMirror e Snapvault per i documenti, coadiuvato anche da Snapshot Copy.

Le copie di backup sono posizionate all'interno della server-farm presso la sede legale e operativa di Archiva S.r.l. in Villafranca di Verona, e replicate all'interno di un proprio ambiente AWS in Cloud, localizzato presso la region "Milano" , con ulteriori repliche, per aspetti di business continuity, presso i poli tecnologici di Cornaredo (MI), Ponte San Pietro (BG) . Archiva ha implementato un processo di gestione dei backup, governato dalla procedura interna "POA.SYS.13 Procedura di gestione dei backup/restore".

Logging e monitoraggio

Archiva mantiene log delle varie componenti che concorrono alla definizione della propria infrastruttura, comprendendo sia apparati di rete, sia elementi software. Archiva ha, inoltre, implementato un sistema di alerting proattivo che notifica ad una distribution list interna, eventuali circostanze rilevanti. I sistemi di monitoraggio e di conseguenza i sistemi di alerting collegati si distinguono in:

- monitoraggi di misure infrastrutturali, dove l'oggetto della misura sono parametri macchina e che consentono quindi misure operate sui sistemi Hardware quali ad esempio Storage, Processi Server, Apparati di Rete, Connettività, Processi Windows e Demoni Java;
- monitoraggio funzionale applicativo, dove l'oggetto della misura sono l'esecuzione di processi funzionali quali ad esempio la richiesta di visualizzazione di un documento, la messa in conservazione di un pacchetto di versamento, la trasformazione di dati, il login di autenticazione ad una applicazione web.

Maggiori dettagli sulla strutturazione del sistema di logging e monitoraggio adottato da Archiva, sono contenuti all'interno della POA 26 Log e Monitoring del SdC.

Clock Syncronization

Tutti i server utilizzati da Archiva S.r.l. a socio unico utilizzano il riferimento temporale offerto dall'I.N.RI.M (Istituto Nazionale di ricerca metrologia) tramite protocollo NTP per la sincronizzazione dei propri orologi.
I clienti di Archiva possono sincronizzare i propri sistemi informativi, utilizzando i medesimi server NTP, elencati all'interno del sito web https://www.inrim.it/node/643

Gestione delle Vulnerabilità tecniche

Al fine di monitorare le vulnerabilità tecniche che nel corso dell'erogazione dei servizi applicativi ai clienti possono manifestarsi, Archiva ha adottato un processo ispirato alla norma ISO 30111:2019 - Information technology — Security techniques — Vulnerability handling processes.
Nel corso di un anno solare, Archiva pianifica almeno 4 sessioni distinte di Vulnerability Assessment sul perimetro esterno, esposto su internet, e scansioni sul perimetro interno. Eventuali vulnerabilità critiche sono immediatamente analizzate e la loro remediation è pianificata entro 15gg.

Misure di Sicurezza

Archiva, nell'esercizio delle attività in qualità di Responsabile del Trattamento, adotta come base line di sicurezza i controlli indicati nell'annex A della ISO/IEC 27001. Tali controlli, estesi anche alle linee guida ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 27701, sono valutati annualmente in occasione degli audit interni e degli audit di terza parte.

Security Operation Center - SOC

Al fine di garantire su base permanente livelli di sicurezza adeguati, Archiva ha implementato un SOC avvelendosi della collaborazione di un fornitore esterno specializzato che monitora H24, 7x7 l'esposizione web dell'azienda, andando ad indagare anche il deep e dark web, al fine di fare emergere eventuali tracce di attività malevole nel darkweb e nel deepweb.

Network Operation Center - NOC

Al fine di garantire su base permanente livelli di sicurezza adeguati, Archiva ha implementato un NOC avvelendosi della collaborazione di un fornitore esterno specializzato che monitora H24, 7x7 tutta l'infrastruttura IT di Archiva, al fine di fare emergere tracce di eventuali anomalie sistemistiche.

Responsabilità e procedure

Il cliente, qualora, nella fruizione dei servizi applicativi, dovesse riscontrare anomalie o rilevare eventi che possono avere ripercussioni sulla sicurezza delle informazioni trattate da Archiva oppure direttamente incidenti di sicurezza delle informazioni, può segnalare ogni circostanza e/o evento scrivendo all'indirizzo email security@pec.archivagroup.it oppure, in alternativa, ciso@archivagroup.it. Ogni richiesta di assistenza relativa alla friuzione dei servizi erogati da Archiva può essere inoltrata tramite portale di ticketing https://archivagroup.atlassian.net/servicedesk/ oppure scrivendo all'indirizzo email ticket.care@archivagroup.it.

Tutte le segnalazioni aperte tramite portale sono tracciate all'interno dei sistemi Archiva con uno specifico ticket. Tutte le segnalazioni di eventi di sicurezza delle informazioni , sono tracciate in apposito registro. Per gli eventi, classificati come incidente di sicurezza delle informazioni, oppure databreach, è disponibile un incident report.

Raccolta di evidenze

Archiva mantiene all'interno dei propri sistemi informativi evidenze della corretta implementazione del sistema di gestione integrato a supporto delle attività in ambito di certificazione. Archiva assicura la massima collaborazione con i clienti per permetter loro di rispondere ad eventuali attività di verifica e ispezione, richieste in prima persona o da autorità di controllo, pur tutelando la riservatezza di particolari aspetti tecnlogici, implementativi e procedurali, propri di Archiva.

Gestione del rischio

Archiva S.r.l ha definito un approccio sistematico alla gestione dei rischi al fine di identificare, analizzare, valutare e g. a socio unico estire i rischi legati alla Riservatezza, Integrità e Disponibilità delle informazioni protette.

La figura del CISO è responsabile di guidare il processo periodico di gestione del rischio.

Report

Il CISO presenta ad Archiva Srl a socio unico una relazione annuale sull'adeguatezza del sistema di protezione e sullo stato di avanzamento dei piani di attuazione. Riporta, inoltre, i risultati degli audit sulla sicurezza delle informazioni.

Audit

Vengono pianificate ed eseguite periodiche attività di audit sulla sicurezza, sulla sicurezza delle informazioni e sul Sistema di Gestione Integrato al fine di:

- rivedere l'adeguatezza dei controlli e l'efficacia del sistema di gestione integrato, individuando possibili miglioramenti;
- verificare l'adeguata attuazione delle politiche e delle regole, individuando possibili situazioni critiche;
- riferire al CEO rilevanti questioni di sicurezza delle informazioni;
- verificare l'efficacia dei sistemi di protezione delle informazioni attraverso la valutazione delle vulnerabilità su sistemi e sulle reti.

Le attività Audit sulla sicurezza delle informazioni sono coordinate dalla figura del CISO.

ISO/IEC 27018 & ISO/IEC 29100 - Principi di Protezione dei Dati

1 - Consent and choice

Archiva, in qualità di Responsabile del Trattamento, come definito nell'atto di designazione sottoscritto con i clienti, si obbliga a supportare il Titolare nel rispetto di ogni suo vincolo regolamentare.

2 - Purpose legitimacy and specification

Il trattamento dei dati operato da Archiva, avviene per le sole finalità e secondo le modalità, concordate con il Titolare, nell'atto di designazione a Responsabile del trattamento.

3 - Collection limitation

Archiva, nel ruolo di Responsabile del trattamento, non ha la facoltà di scegliere l'insieme dei dati personali da trattare, poiché questi vengono forniti direttamente dal Titolare del trattamento (Cliente).

4 - Data minimization

Archiva si impegna ad utilizzare solamente i dati strettamente necessari per le finalità dichiarate e ad eliminare dai propri sistemi informativi eventuali file temporanei o documenti di lavoro, non più necessari al trattamento dei dati del Titolari.

5 - Use, retention and disclosure limitation

Archiva prevede la possibilità di dare accesso ai dati del Titolare, su richiesta delle autorità di controllo competenti, senza ritardarne l'accesso ed informando tempestivamente il Titolare, così come previsto nell'atto di designazione a Responsabile del trattamento. Di questa diffusione viene tenuta traccia in apposita documentazione.

6 - Openness, transparency and notice

Archiva rende noto l'eventuale ricorso ad ulteriori responsabili (come identificati all'Art. 28, comma 4 del Regolamento UE 2016/679), comunicando il loro coinvolgimento, nell'atto di designazione a Responsabile del trattamento.

7 - Accountability

Archiva, in qualità di Responsabile del Trattamento, si obbliga a notificare al Titolare eventuali violazioni dei dati personali di sua pertinenza, secondo le modalità e le tempistiche definite nell'accordo di designazione a Responsabile del Trattamento. In caso di Data Breach Archiva redige uno specifico rapporto la cui struttura corrisponde a quanto indicato all'art. 33 del Regolamento (UE) 2016/679.

Al fine di supportare nel tempo eventuali indagini forensi, Archiva mantiene all'interno dei propri sistemi informativi copia aggiornata e storicizzata di tutte le politiche, procedure e istruzioni operative necessarie all'esercizio del Sistema di Gestione Integrato.

Qualora il Titolare richiedesse la restituzione dei propri asset informativi (i documenti conservati all'interno del SdC) Archiva applicherà quanto
previsto nella procedura POA 01 - Gestione dello Scarto dal Sistema di Conservazione.

8 - Information security

- tutto il personale dipendente ed eventuali collaboratori di Archiva, sono soggetti a specifici accordi di riservatezza;
- al fine di prevenire la copia non autorizzata di informazioni su dispositivi mobili o trasportabili, Archiva adotta meccanismi di DLP, che segnalano tempestivamente eventuali tentativi di copia non autorizzata;
- tutte le attività di Restore dei dati sono tracciate in appositi log applicativi;
- i dati trasmessi dal Titolare non sono memorizzati su dispositivi mobili o rimovibili, eccezion fatta per i casi in cui sia il Titolare a richiedere una copia su supporto ottico di tali dati. In queste circostanze i dati vengono memorizzati all'interno di directory compresse e protette con password robuste, comunicate al Titolare con canali di comunicazione differenti rispetto quello impiegato per la trasmissione dei dati;
- tutti i dati in transito, fra Titolare e Archiva, sono scambiati attraverso canali di comunicazione cifrati (SSL/TLS1.2);
- la distruzione degli originali analogici o delle loro copie, trasmesse dai Titolari, avviene per mezzo di un sub-fornitore contrattualizzato, che esegue il servizio di "macero carta", certificato;
- ogni utente che accede ai sistemi informativi di Archiva, attraverso i quali sono erogati i servizi di business ai Titolari, utilizza credenziali di autenticazione uniche, non generiche non tecniche;
- periodicamente è riesaminata la lista delle utenze autorizzate ad accedere al Sistema di Conservazione;
- le utenze scadute e/o disattivate, non vengono riassegnate ad altri utenti;
- l'atto di designazione a Responsabile del trattamento, indica le misure minime di sicurezza implementate da Archiva, nell'erogazione dei propri servizi;
- le misure tecniche organizzative concordate fra Titolare e Archiva sono estese, laddove pertinente, agli eventuali ulteriori responsabili coinvolti nel trattamento;
- l'eventuale riuso di dispositivi di memorizzazione di massa avviene solo a seguito di cancellazione profonda del filesystem del supporto;
- Archiva tratta i dati personali dei Titolari, esclusivamente all'interno del territorio nazionale, presso la sede di Villafranca di Verona (VR).

Questo documento non può essere duplicato o diffuso senza l'esplicito consenso scritto di Archiva S.r.l. a socio unico. Qualsiasi divulgazione, anche parziale, delle informazioni contenute nel presente documento che non sia stata preventivamente autorizzata da Archiva S.r.l. a socio unico può costituire una violazione di legge. Per qualsiasi richiesta, si prega di contattare ciso@archivagroup.it.