Sintesi_Politica di Cybersecurity e Sicurezza delle Informazioni del Gruppo PLC

Sommario

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

1 Premessa, principi ispiratori ed obiettivo

PLC S.p.A. e le società da essa controllate direttamente e/o indirettamente (il "**Gruppo PLC**") riconosce che le informazioni, in tutte le loro forme, rappresentano un asset primario e strategico. La protezione delle informazioni e dei sistemi ICT è fondamentale per garantire la continuità operativa, la tutela dei dati personali e il rispetto delle normative vigenti, in particolare la Direttiva (UE) 2022/2555 (NIS2) e il D.Lgs. 138/2024, ragion per cui PLC considera di fondamentale importanza porsi l'obiettivo di orientare l'intera organizzazione e i propri stakeholders verso una gestione della cybersecurity e la sicurezza delle informazioni, nel pieno rispetto dei requisiti normativi sopra indicati e degli standard internazionali in materia.

2 Ambito di applicazione

La Politica si applica a:

- tutte le risorse informative e tecnologiche del Gruppo PLC, incluse quelle gestite da fornitori e outsourcer;
- dipendenti, collaboratori, consulenti, visitatori e terze parti che accedono ai sistemi informativi;
- tutte le informazioni trattate dai sistemi aziendali, in qualsiasi forma e durante tutto il ciclo di vita.

3 Obiettivi strategici

- **Riservatezza**: garantire che le informazioni siano accessibili solo a soggetti autorizzati;
- **Integrità**: assicurare la completezza e l'autenticità delle informazioni;
- **Disponibilità**: garantire l'accesso alle informazioni quando necessario;
- **Verificabilità e accountability**: tracciare le operazioni e attribuire le responsabilità nella gestione;
- **Autenticità**: assicurare la certezza dell'identità di utenti e sistemi;
- **Continuità operativa**: minimizzare i rischi e garantire la resilienza dei servizi essenziali.

4 Modello organizzativo e governance

La governance della sicurezza delle informazioni è strutturata su più livelli, di cui di seguito le figure chiave:

- **Consiglio di Amministrazione (CdA):** In qualità di organi amministrativi e direttivi, ai sensi dall'art.23 del D. Lgs. 138/2024, i componenti degli organi amministrativi sono individuati quali "Responsabili delle violazioni NIS". Nell'ambito del Sistema di gestione per la Cybersecurity e la Sicurezza delle Informazioni, il CdA assume altresì il ruolo di "Direzione" ai sensi del citato decreto;

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

- **Chief Information Security Officer (CISO):** Presidia le tematiche di Cybersecurity e Sicurezza delle Informazioni, governa e monitora l'attuazione del Sistema di gestione per la Cybersecurity e la Sicurezza delle Informazioni e nel quadro degli obblighi derivanti dall' art 7 co.1 lettera c, del D. Lgs.138/2024, è il "Punto di Contatto NIS" per i rapporti con l'Agenzia per la Cybersicurezza Nazionale (ACN). Nel Gruppo PLC il CISO è il Responsabile del dipartimento ICT, e coincide con il ruolo del CIO, ovvero colui che è responsabile della strategia e della gestione delle tecnologie dell'informazione e dei sistemi informatici dell'organizzazione per il raggiungimento degli obiettivi di business;

- **Referente Privacy**: garantisce l'attuazione del **Sistema di gestione Privacy** adottato da PLC in conformità al GDPR, alla vigente normativa nazionale e alle altre disposizioni del Garante relative alla protezione dei dati. In PLC il ruolo è ricoperto dal Responsabile del dipartimento "Affari Legali e Societari";
- **Comitato per la Cybersecurity**: organo interfunzionale che definisce la strategia, valuta i rischi e promuove la cultura della sicurezza;
- **Referente CSIRT**: gestisce le notifiche di incidenti significativi verso le autorità competenti. Nel Gruppo PLC la funzione è ricoperta dalle risorse in forza al dipartimento ICT. **Ruoli di management**: includono Cybersecurity Implementer, Amministratore di sistema, HR Security Manager, Physical Security Manager, Third Parties Security Manager, Information User, Process Owner, User Manager.

5 Principi generali

Di seguito sono elencati i principi a cui è ispirata la Politica in materia di Cybersecurity e di Sicurezza delle Informazioni.

P1 – Responsabilità individuale

Ogni individuo, interno o esterno al Gruppo PLC, è responsabile delle sue azioni in conformità con il relativo contratto e/o con le procedure e le normative interne adottate dal Gruppo PLC.

P2 – Utilizzo degli strumenti informatici aziendali

I beni forniti ai dipendenti per l'esecuzione delle proprie attività lavorative sono di proprietà delle società del Gruppo PLC (il cui uso è strettamente permesso per le sole finalità connesse al lavoro). I beni non di proprietà dell'azienda utilizzati per finalità connesse al lavoro devono essere comunque autorizzati e configurati dell'azienda per garante la conformità alle politiche di sicurezza adottate dal Gruppo PLC.

P3 – Identificazione delle informazioni necessarie al Ruolo

Ogni individuo del Gruppo PLC e ciascun stakeholder viene autorizzato ad accedere alle sole informazioni strettamente attinenti alla sua mansione lavorativa e/o necessarie per l'esecuzione del proprio contratto; le procedure

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

e le istruzioni operative informatiche vengono sviluppate e configurate per raggiungere questo obiettivo e limitare l'accesso a dati non necessari per l'attività del singolo utente.

P4 – Identificazione delle attività

Nell'accedere ai sistemi informatici, ogni individuo viene autorizzato a svolgere solo le attività strettamente connesse al suo lavoro e solamente per il periodo temporale necessario.

P5 – Disponibilità delle informazioni e dei Sistemi Informativi

La disponibilità delle Informazioni e dei Sistemi Informativi è un pilastro della sicurezza informatica (parte della triade CIA: Confidenzialità, Integrità, Disponibilità), che assicura che utenti autorizzati possano accedere a dati e sistemi necessari in qualsiasi momento, in modo tempestivo e affidabile, secondo le esigenze di business.

P6 – Separazione dei Compiti

A fine di garantire che nessun individuo abbia il controllo esclusivo su una specifica componente informativa o di un processo, ci deve essere una reale e durevole separazione di autorità e responsabilità (c.d. segregation of duties).

P7 – Proporzionalità

Le misure di sicurezza devono essere individuate e realizzate in proporzione al rischio, al valore del patrimonio informativo che intendono proteggere ed alle esigenze normative.

P8 – Mantenimento di Affidabilità

La sicurezza informatica, all'interno del Gruppo PLC, deve essere attuata a un livello tale da non comprometterne l'affidabilità dei dati, dei sistemi e delle reti.

P9 – Sicurezza nella Progettazione

Gli aspetti di sicurezza e di trattamento delle informazioni personali devono essere considerati durante le fasi di progettazione di ogni componente informatica. Le soluzioni temporanee sono adottate nei soli casi strettamente necessari.

P10 – Prudenza

Le reti informatiche ed i sistemi esterni al Gruppo PLC, in via prudenziale, devono essere considerati alla stregua delle reti insicure (untrusted).

P11 – Integrità

L'informazione può essere modificata solo previa autorizzazione del responsabile della stessa individuato alla luce del Dipartimento competente e della struttura aziendale. Il Gruppo PLC si impegna alla corretta e trasparente

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

determinazione del responsabile dell'informazione.

P12 – Riservatezza

L'informazione non deve essere rivelata ad entità che fanno parte del sistema (utenti, processi, dispositivi) a meno che questi non siano stati autorizzati ad accedere o sia necessario che accedano alla medesima informazione al fine di poter svolgere le loro mansioni.

6 Obiettivi

Il Gruppo PLC garantisce la cybersecurity e la sicurezza delle informazioni in conformità alle normative vigenti e agli standard internazionali in materia nel pieno rispetto dei requisiti da essi indicati.

Per raggiungere tale risultato, il Gruppo PLC considera di fondamentale importanza orientare l'organizzazione (interna ed esterna) verso una gestione della cybersecurity e la sicurezza delle informazioni che si allinei al contesto dei rischi ICT. In tal senso, PLC garantisce un adeguato livello di protezione del proprio sistema informativo e il perseguimento degli obiettivi strategici di seguito indicati.

O1 – Politica per la Cybersecurity e la Sicurezza delle Informazioni

Predisporre e tenere aggiornata la Politica di Cybersecurity e Sicurezza delle Informazioni che fornisce le linee di indirizzo strategico sui domini della sicurezza al fine di garantire la protezione degli asset e dei servizi aziendali dai rischi cyber e il rispetto degli obblighi vigenti (legali, contrattuali e delle normative interne).

O2 – Organizzazione della Cybersecurity e della Sicurezza delle Informazioni

Definire ruoli e responsabilità del personale coinvolto nella gestione della Cybersecurity e della Sicurezza delle Informazioni, tenendo in considerazione i principi di segregazione dei ruoli e le linee di riporto gerarchico per l'attuazione delle misure di sicurezza e la gestione dei rischi relativi. Definire gli adeguati flussi informativi interni e verso le autorità pubbliche o i gruppi di interesse, per far fronte con rapidità, efficacia e scrupolo a emergenze o incidenti che possano verificarsi nello svolgimento delle attività, collaborando anche con terze parti o Enti preposti.

O3 – Sicurezza nel processo di gestione delle risorse umane

Istruire ogni utente adibito al trattamento dei dati e allo svolgimento di operazioni critiche (amministratori di sistema e utenti con abilitazioni privilegiate) che opera in azienda o per suo conto in servizi esternalizzati in materia di requisiti di Cybersecurity e di Sicurezza delle Informazioni. Assicurare che la gestione della Cybersecurity e della Sicurezza delle Informazioni sia parte integrante dei processi di inserimento, entrata, permanenza e fuoriuscita dei dipendenti. Assicurare in caso di cessazione o variazione del rapporto di lavoro, la tempestiva rimozione delle autorizzazioni agli accessi (o modifiche in caso di variazioni di appartenenza a strutture organizzative interne o incarico) e la restituzione

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

degli asset assegnati al Gruppo PLC.

O4 – Asset Management

Identificare, classificare, censire e documentare le informazioni aziendali, gli asset associati e le strutture di elaborazione delle stesse. Identificare, documentare e attuare le regole per l'utilizzo, la gestione, la restituzione e la dismissione/distruzione degli asset e/o dei dispositivi. Prevedere misure di sicurezza aggiuntive per gli asset che memorizzano ed elaborano informazioni e dati personali, utilizzati all'esterno della Società (es. in caso di smart working).

O5 – Sicurezza logica e controllo degli accessi

Implementare un processo formale di accreditamento per l'accesso logico a reti e sistemi informatici, basato sulle effettive necessità operative (principio del minimo privilegio) e sulle normative e sugli obblighi contrattuali riguardanti le limitazioni per l'accesso delle informazioni. Prevedere procedure di autenticazione rafforzate per le attività operative critiche. Accordare i diritti di accesso, di norma, previa formale autorizzazione rilasciata a personale qualificato per la specifica operatività, mediante ricorso ad opportuni profili abilitativi. Monitorare periodicamente e possibilmente continuamente, gli accessi alle reti e ai sistemi informatici, soprattutto se relativi a operazioni critiche o alle attività degli amministratori di sistema.

O6 – Sicurezza delle Reti

Salvaguardare la riservatezza e l'integrità dei dati in transito su reti private, pubbliche o su reti wireless tramite controlli speciali al fine di prevenire l'accesso non autorizzato. Definire, realizzare o controllare (nel caso di servizi esternalizzati) le misure di sicurezza necessarie a garantire adeguati meccanismi di protezione delle informazioni sull'architettura hardware e software di rete e il monitoraggio delle infrastrutture di rete, della rete aziendale interna (LAN), della rete wireless e delle connessioni con le società del Gruppo PLC ed i propri fornitori.

O8 - Crittografia

Definire i criteri per l'adozione dei controlli crittografici e formalizzare una istruzione operativa per l'utilizzo, la protezione e la durata delle chiavi crittografiche in funzione della valutazione dei rischi condotta, della proporzionalità dei controlli applicati (o applicabili) e della normativa applicabile. Per la definizione dei suddetti criteri deve essere considerato l'impatto dell'utilizzo di informazioni crittografate sui controlli basati sull'ispezione dei contenuti (ed es. identificazione malware, spyware, etc.).

O9 – Sicurezza fisica

Garantire solo al personale autorizzato l'accesso alle sedi ed ai singoli locali aziendali, al fine di prevenire la perdita, il danneggiamento, la compromissione di asset o l'interruzione delle attività operative. Garantire la sicurezza delle informazioni e delle risorse informatiche attraverso misure di sicurezza fisica la cui intensità è graduata in relazione

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

alle risultanze della valutazione del rischio e alla classificazione delle risorse. Proteggere le risorse informatiche da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti delle infrastrutture di supporto (ad es. telecomunicazioni, riscaldamento /ventilazione e condizionamento dell'aria) e garantire la loro continuità e integrità attraverso una corretta manutenzione.

010 – Sicurezza nell'operatività

Garantire la sicurezza e la correttezza delle informazioni all'interno delle attività operative e di quelle a supporto, attraverso la strutturazione di un framework di procedure documentato con riguardo a: elaborazione e trattamento delle informazioni e dei dati personali; attività di change management sui sistemi informativi; sostenibilità in termini di capacità dei sistemi informativi con le esigenze vigenti e future; riavvio dei sistemi e procedure di ripristino nel caso di malfunzionamenti di sistema; attività di backup; attività di controllo per l'individuazione, la prevenzione e il ripristino inerenti ai malware; registrazione, gestione e monitoraggio dei log degli eventi e delle attività degli utenti; installazioni e configurazione di sistemi e applicazioni informatiche; gestione delle vulnerabilità tecniche dei sistemi informativi; inventario o mappa del patrimonio ICT; identificazione e pianificazione dei requisiti e delle attività di audit sui sistemi informativi, al fine di minimizzare le interferenze con i processi di business.

O11 – Sicurezza nelle comunicazioni

Assicurare l'adeguata gestione delle reti di telecomunicazione aziendali e la protezione dei servizi ad esse relativi, attraverso controlli che definiscano le misure di sicurezza adottate, la segregazione e la segmentazione delle reti in linea con la criticità delle informazioni di business interessate. Le misure di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inseriti negli SLA con i fornitori di tali servizi. Garantire la sicurezza nel trasferimento delle informazioni. Prevedere accordi di riservatezza e "non-disclosure" in caso di scambio di informazioni.

O12 – Acquisizioni dei sistemi, sviluppo e manutenzione

Definire i requisiti di sicurezza e assicurare adeguati controlli durante le fasi di acquisizione, progettazione, sviluppo ed utilizzo dei sistemi informativi aziendali. In particolare, nel ciclo di sviluppo del software devono essere considerati anche gli aspetti inerenti al trattamento dei dati personali, adottando pertanto un approccio c.d. "Security & Privacy by Design e by Default". Nel caso di sviluppo affidato all'esterno, supervisionare e monitorare la conformità delle attività del fornitore con i requisiti di sicurezza definiti dal Gruppo PLC.

O13 – Relazioni con i fornitori ICT

Garantire le misure di mitigazione dei rischi ICT e di sicurezza anche quando i servizi e/o i sistemi ICT sono esternalizzati o quando si ricorre all'utilizzo di terze parti. Mantenere la piena responsabilità di quanto compiuto dal fornitore di servizi verso il quale si sono esternalizzate funzioni operative o aziendali. Adottare misure adeguate affinché sia garantito il rispetto da parte del fornitore di quanto previsto dalla presente Politica e dalla normativa

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

cogente in tema di cybersecurity e protezione dei dati. Includere nella fase di qualifica e negli accordi contrattuali con i fornitori i requisiti di cybersecurity e sicurezza delle informazioni derivanti dall'analisi dei rischi e dalle normative cogenti cui l'azienda è obbligata ad adempiere, assicurandosi che i fornitori estendano i suddetti requisiti di sicurezza nei confronti dei sub fornitori eventualmente coinvolti.

O14 – Gestione degli incidenti di sicurezza Informatica

Garantire, tramite modalità strutturate, le attività di monitoraggio degli eventi nell'ambito della sicurezza informatica e la relativa classificazione, considerando anche nuove minacce e vulnerabilità. Definire i ruoli, le responsabilità, le procedure e le istruzioni operative di gestione degli incidenti di sicurezza informatica. Definire e documentare i flussi di comunicazione interna ed esterna in caso di incidenti che comportino rischi di interruzione della continuità operativa e regolamentare la segnalazione alla struttura preposta a dichiarare lo stato di crisi. Disciplinare e documentare i processi di segnalazione degli incidenti di sicurezza "Significativi" alla competente Autorità nazionale, con osservanza delle metodologie e dei processi di informativa normate da ACN.

O15 – Aspetti di sicurezza Informatica in tema di disponibilità delle informazioni e Continuità Operativa

I servizi, i processi e i sistemi devono essere implementati e gestiti assicurando una solida gestione della continuità operativa allo scopo di massimizzare la capacità di prestare servizi su base continuativa e di limitare le perdite in caso di gravi interruzioni dell'operatività. Garantire la definizione, revisione ed eventuale e aggiornamento periodico del piano di "Continuità Operativa e di Disaster Recovery", e dei relativi allegati. L'aggiornamento è effettuato sulla base dei risultati delle verifiche, delle informazioni sulle minacce correnti, della condivisione delle informazioni, dei mutevoli obiettivi di ripristino e delle analisi degli scenari operativamente e tecnicamente plausibili non ancora verificatisi, nonché, se del caso, a seguito di modifiche sui sistemi e sui processi.

O16 – Compliance

Adottare un processo di monitoraggio normativo che garantisca il tempestivo adeguamento aziendale alle disposizioni normative e regolamentari in materia di cybersecurity. Garantire il controllo e il riesame periodico e complessivo delle istruzioni operative in materia di Cybersecurity e di Sicurezza delle Informazioni.

O17 – Normativa interna

Pubblicare, diffondere, informare e aggiornare la documentazione aziendale che dettagli le regole di "Cybersecurity e di Sicurezza delle Informazioni" adottate da PLC e a cui tutti i dipendenti possono accedere e devono attenersi. Documentare i ruoli e le responsabilità connessi alla gestione della cybersecurity, con diretto collegamento all'organigramma aziendale per l'identificazione delle linee di riporto gerarchico per l'attuazione delle misure di sicurezza. Riesaminare periodicamente i sistemi informativi per garantire la conformità con le politiche e con gli standard di sicurezza aziendali.

7 Requisiti e linee guida strategiche

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

La Politica prevede:

- gestione strutturata del rischio secondo standard ISO/IEC 27001, NIST CSF e linee guida ENISA;
- adozione di procedure per la sicurezza nella gestione delle risorse umane, asset management, controllo degli accessi, gestione delle password, sicurezza fisica e logica, gestione delle vulnerabilità, patch management, change management;
- protezione delle reti, delle applicazioni e dei database, con particolare attenzione alla segmentazione, alla crittografia e al monitoraggio degli eventi di sicurezza;
- gestione degli incidenti di sicurezza, con processi di segnalazione, risposta, analisi post-incidente e comunicazione verso le autorità;
- svolgimento di audit periodici, monitoraggio continuo e miglioramento del sistema di gestione della sicurezza.

8 Compliance normativa

La Politica recepisce e integra a titolo esemplificativo:

- Direttiva NIS2;
- D.Lgs. 138/2024;
- Legge 90/2024;
- GDPR;
- D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101 (Codice Privacy);
- Standard internazionali (ISO/IEC 27001, NIST, UNI/PdR 174);
- Regolamenti e politiche interne tra cui: Codice Etico, Modello di Organizzazione, Gestione e Controllo 231, Politica di Gruppo Anticorruzione, Social Media Policy, Water Policy, Politica di Gruppo Salute, sicurezza e ambiente, Politica di Gruppo Global Quality, Procedura per il trattamento delle Informazioni Privilegiate, Politica sulla Protezione dei dati Personali.

9 Disciplina delle violazioni della Politica

Il mancato rispetto della Politica Cybersecurity e di Sicurezza delle Informazioni da parte del personale dipendente prevede l'applicazione di provvedimenti disciplinari nei confronti del soggetto responsabile, mentre nei confronti degli stakeholders sono previste discipline contrattuali ad hoc. Gli eventuali provvedimenti nei confronti del personale interno sono riconducibili a quanto regolamentato nel Contratto Collettivo Nazionale del Lavoro (CCNL) adottato dal Gruppo PLC.

10 Aggiornamento e comunicazione

La Politica è stata emanata ed approvata nella sua prima edizione il 10 dicembre 2025 e sarà soggetta a revisione periodica, audit e aggiornamento in base all'evoluzione normativa, tecnologica e organizzativa. Il dipartimento ICT coordina e gestisce la redazione e l'aggiornamento della presente Politica, la stessa è sottoposta all'approvazione del

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.

Consiglio di Amministrazione, previo parere del Comitato Controllo Rischi e Sostenibilità. La Politica è comunicata a tutto il personale e alle terze parti coinvolte nella gestione delle informazioni e resa disponibile in estratto sul sito istituzionale del Gruppo PLC.

Questo documento è di proprietà di PLC S.p.A. che ne conserva tutti i diritti.