

# Politica sulla sicurezza delle Informazioni e dei Servizi Cloud

## Security Policy

### Scopo

La politica di sicurezza delle informazioni, dei dati personali e della conservazione digitale ha l'obiettivo di proteggere le risorse informative da ogni tipo di minaccia, sia essa di natura organizzativa o tecnologica, interna o esterna, accidentale o intenzionale, garantendo la riservatezza, l'integrità, la disponibilità delle informazioni e il rispetto della normativa vigente.

In questo ambito, PRT S.p.A. stabilisce i principi per assicurare la sicurezza delle informazioni trattate attraverso servizi cloud, quando opera come fornitore di soluzioni rivolte ai clienti finali, basate su infrastrutture e tecnologie messe a disposizione da Cloud Service Provider (CSP).

La politica è conforme agli standard internazionali ISO/IEC 27017 e ISO/IEC 27018, con l'obiettivo di tutelare i dati aziendali e quelli dei clienti finali, preservandone la riservatezza, l'integrità e la disponibilità.

### Politica di sicurezza

La Direzione dell'azienda definisce la sua politica aziendale finalizzata a:

- Garantire la riservatezza e integrità delle informazioni e dei dati personali, impedendo che estranei non autorizzati ne abbiano accesso, garantendo che le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi elaborativi forniscano le prestazioni elaborative ai livelli e con i requisiti definiti;
- Rispettare i requisiti normativi, legislativi sulla protezione dei dati e delle informazioni e le regole interne, usando i dati in modo lecito e secondo correttezza, cioè in armonia con le leggi, i regolamenti e nel rispetto della lealtà e della trasparenza del trattamento;
- Adottare misure di sicurezza e di controllo degli accessi fisici, che prevedono le seguenti classi di accesso: personale dell'organizzazione; personale di fornitori esterni; personale dell'amministrazione servite dal sistema di conservazione. Avendo riguardo alla natura



---

dei dati, cioè a seconda del loro carattere “sensibile” o meno, e alle specifiche caratteristiche del trattamento;

- Custodire e controllare i dati personali oggetto del trattamento, in conformità al GDPR, in modo che sia minimizzato e ricondotto ad una soglia di rischio accettabile il rischio di distruzione o perdita, anche accidentale, degli stessi;
- In qualità di fornitore PRT S.p.A. si impegna a richiedere ai CSP trasparenza in merito a ubicazione dei dati, utilizzo di subfornitori e misure di protezione dei dati personali, trasferendo tali garanzie ai propri clienti finali. Nei contratti con i clienti prevedere clausole esplicite sulla protezione dei dati personali, sulla gestione degli accessi e sulle modalità di notifica in caso di violazioni.
- Assicurare la gestione delle postazioni di lavoro, i cui elementi essenziali possono essere: regole per l’installazione del software sulle postazioni di lavoro, regole per gli aggiornamenti, regole per la limitazione della connettività a supporti esterni (CD/DVD; Pen Drive, ecc), regole per la modifica delle impostazioni;
- Garantire la manutenzione dei sistemi, il controllo sul contenuto software dei client al fine di verificare l’assenza di codice malevolo e la conformità a quanto autorizzato e previsto dalle licenze d’uso;
- Garantire la cyber security attraverso l’aggiornamento continuo dei sistemi di sicurezza, la formazione specifica del personale e la stipula di un’apposita polizza assicurativa al fine di garantire la continuità d’impresa;
- Garantire la gestione degli apparati mobili (portatili, tablet, smartphone, cellulari, ecc) e dei supporti esterni ai server e alle postazioni di lavoro, che siano prodotti nell’ambito delle attività di conservazione digitale;
- Garantire un piano di continuità aziendale attraverso le misure di business continuity e disaster recovery messe a disposizione dai CSP. In qualità di fornitore, verificare che i CSP abbiano predisposto piani efficaci e periodicamente testati, e assicurare che tali garanzie siano riportate negli accordi stipulati con i clienti finali.
- Controllare i canali di comunicazione, quali e-mail, sistemi di instant messaging, VoIP, internet, accessi wireless, fax, scanner, fotocopiatrici, al fine di preservare la confidenzialità, e l’integrità delle informazioni in transito, ed allo stesso tempo ad impedire l’abuso che si potrebbe fare di tali strumenti di comunicazione. Di conseguenza la tipologia di controlli deve coprire le problematiche di utilizzo appropriato dello strumento, le problematiche di comportamento dell’utilizzatore dello strumento e le tecnologie coinvolte;

- 
- Garantire al personale ed ai collaboratori una adeguata conoscenza e grado di consapevolezza dei problemi connessi con la sicurezza dell'informazione al fine di acquisire sufficiente coscienza delle loro responsabilità in merito al suo trattamento;
  - Accertare che tutti i fornitori esterni abbiano consapevolezza dei problemi di sicurezza delle informazioni e rispettino la politica adottata dall'azienda;
  - Prevedere il perfezionamento, la divulgazione e il riesame delle politiche di sicurezza al verificarsi dei seguenti casi: incidenti di sicurezza, variazioni tecnologiche significative, modifiche all'architettura informatica, aggiornamenti delle prescrizioni normative (anche legate alla conservazione digitale), risultati delle eventuali attività di audit interni;
  - Garantire la long preservation e l'obsolescenza dei formati per quanto attiene la gestione dei documenti oggetto di conservazione digitale;
  - Monitorare i sistemi e i processi attraverso apposite verifiche e rilevare indicatori che possano essere utilizzati a migliorare l'efficienza e a valutare il raggiungimento degli obiettivi prefissati;
  - Monitorare i propri ambienti cloud e registrare gli accessi e gli eventi di sicurezza. In qualità di fornitore, PRT S.p.A. effettuare verifiche periodiche sui Cloud Service Provider (CSP), tramite certificazioni ISO/IEC 27001, 27017, 27018. Mantenere meccanismi di controllo per garantire la conformità dei servizi ai requisiti di sicurezza e privacy.
  - Migliorare costantemente i propri servizi fissando obiettivi raggiungibili nel breve e medio periodo per garantire sempre livelli di eccellenza ai propri clienti;
  - Garantire un continuo aggiornamento dei sistemi e del know how degli operatori rispetto all'evoluzione tecnologica e alle innovazioni informatiche e dei sistemi di sicurezza connessi. Aggiornare costantemente l'analisi dei rischi rispetto ai pericoli emergenti connessi all'utilizzo delle nuove tecnologie ed introdurre misure di sicurezza specifiche, proporzionate rispetto ai rischi stessi;
    - Diffondere e promuovere una cultura, una conoscenza dei sistemi aziendali e una consapevolezza della sicurezza informatica a tutti i livelli aziendali.
    - Utilizzare strumenti di threat intelligence per raccogliere dati sulle minacce attuali e potenziali tramite l'analisi delle informazioni per identificare tendenze e pattern di attacco.
    - Migliorare le pratiche di sicurezza in tutte le fasi del ciclo di vita dello sviluppo (SDLC), dalla pianificazione al rilascio e garantire l'utilizzo di ambienti di test separati dalla produzione.



---

La politica di sicurezza delle informazioni è attuata per proteggere ad un livello ottimale il sistema di gestione delle informazioni e della privacy da eventi intesi come minacce o incidenti, esterni e/o interni oggettivi e/o soggettivi, che possono compromettere l'erogazione dei servizi. In tutto ciò la Direzione si impegna ad assumere un ruolo attivo costante e di sostegno nella promozione e guida di tutte le attività aventi influenza sulla sicurezza delle informazioni.

L'azienda PRT S.p.A. si impegna inoltre a preservare la riservatezza, l'integrità e la disponibilità di tutte le informazioni (in formato elettronico e non) in tutta l'organizzazione al fine di mantenere il proprio vantaggio competitivo, solidità economica, redditività, conformità legale e contrattuale e immagine commerciale. Le informazioni ed i requisiti di sicurezza delle informazioni continueranno ad essere allineati con gli obiettivi aziendali ed il Sistema di Gestione per la Sicurezza delle Informazioni è destinato a essere un meccanismo di abilitazione della condivisione delle informazioni per l'operatività della Società e per ridurre i rischi relativi alle informazioni a livelli minimi accettabili. Tutti i dipendenti dell'organizzazione sono tenuti a rispettare le presenti politiche e l'intero

Sistema di Gestione per la Sicurezza delle Informazioni. Anche alcune terze parti, individuate dalla Direzione generale, saranno tenute a rispettarle. La politica sarà riesaminata ogni qualvolta sarà necessario e comunque mediamente una volta all'anno. La presente politica riguarda la gestione e l'utilizzo del sistema informativo in tutti i suoi aspetti. Per perseguire gli obiettivi aziendali, le informazioni devono soddisfare determinati requisiti:

- **riservatezza:** le informazioni devono essere conosciute solo da coloro che ne hanno il relativo diritto, rispettando il principio del minimo privilegio ("necessità di sapere") in base alle mansioni ricoperte ("necessità di operare");

- **integrità:** le informazioni devono essere precise e complete, devono rispettare i valori e le aspettative aziendali, e devono essere protette da modifiche e cancellazioni non autorizzate. Per soddisfare tale requisito le informazioni devono essere esatte, aggiornate e leggibili;

- **disponibilità:** le informazioni devono essere disponibili quando richiesto dai processi aziendali, in maniera efficiente ed efficace;

- **efficacia:** le informazioni devono essere rilevanti e pertinenti al processo aziendale e, allo stesso tempo, devono essere disponibili tempestivamente, senza errori e fornite in modo da poter essere utilizzate.

- **efficienza:** le informazioni devono essere fornite attraverso l'uso ottimale delle risorse sia dal punto di vista della produttività che della economicità;

---

- **affidabilità:** le informazioni devono essere appropriate, in modo da permettere ai vertici aziendali di gestire l'azienda e garantire la corretta assunzione delle decisioni; allo stesso modo le informazioni fornite ai responsabili delle varie funzioni devono permettere loro di espletare le loro funzioni, gli obblighi di produzione del bilancio e tutti i report e relazioni previste dalla normativa interna ed esterna.

Particolare attenzione verrà posta la gestione degli incidenti di sicurezza informatica tramite specifica procedura formalmente definita.

L'obiettivo è quello di minimizzare l'impatto di eventi avversi e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolte. Tale procedura individua le funzioni a cui comunicare gli incidenti secondo un'opportuna procedura di escalation.

L'attenta valutazione degli incidenti informatici avvenuti sarà motivo di rivalutazione e revisione periodica e/o immediata e tempestiva della presente *security policy*.

Beinasco, 06/11/2025

Il Direttore Generale  
Ing. Riccardo Pesce

