PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

Politica di Sicurezza per il Modello di Responsabilità Condivisa (Shared Security Responsibility Model) - SSRM

Revisione 01 del 26/05/2026

	EMESSO	APPROVATO
Funzione	**Responsabile Gestione Sicurezza delle Informazioni**	**Amministratore Delegato**
Data	26/05/2026	26/05/2026
Firma		

INDICE

1. RIFERIMENTI NORMATIVI

- 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)
- DECRETO LEGISLATIVO 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)
- DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 Luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei Sistemi informative nell'Unione
- DECRETO LEGISLATIVO 18 maggio 2018, n. 65, recante: "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione";
- DECRETO-LEGGE 14 giugno 2021, n. 82 convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.
- ***Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS2), che abroga la Direttiva (UE) 2016/1148.***
- ***Decreto legislativo 4 settembre 2024, n. 138, recante "Recepimento della direttiva (UE) 2022/2555 […] c.d. decreto NIS", che abroga il D.lgs. 18 maggio 2018, n. 65.***
- ***Determinazione del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale n. 379907 del 19 dicembre 2025 (in vigore dal 15 gennaio 2026), che stabilisce, in fase di prima applicazione, le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli artt. 23, 24, 25, 29 e 32 del decreto NIS – Allegato 2 "Misure di sicurezza di base per i soggetti essenziali" e Allegato 4 "Incidenti significativi di base per i soggetti essenziali".***
- ***Framework Nazionale per la Cybersecurity e la Data Protection, edizione 2025, elaborato dal CIS Sapienza e dal CINI in collaborazione con ACN.***
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information and privacy protection — Information security management systems — security management systems —Requirements
- Security Policy di Gruppo
- Politiche e procedure del Sistema di Gestione della Sicurezza delle Informazioni:
    i. Politica della Sicurezza delle Informazioni
    ii. Politica per la Continuità Operativa
    iii. Politica per la gestione dei servizi IT
    iv. Politica per la Gestione degli incidenti di sicurezza delle informazioni

v. Piano di gestione degli incidenti di sicurezza delle informazioni
vi. Piano di risposta agli incidenti di sicurezza delle informazioni
vii. Piano di Gestione dei Servizi
viii. Business Service Catalogue (Catalogo dei Servizi)
ix. POI SI 01 - Metodologia analisi dei rischi
x. POI SI.02 - Gestione log
xi. POI SI 03 - Gestione accessi fisici e logici
xii. POI SI 04 - Comunicazione e operazioni
xiii. POI SI 05 - Gestione incidenti
xiv. POI SI 06 - Business continuity
xv. POI SI 07 - Procedura per Utenti
xvi. POI SI 08 - Procedura per IT
xvii. POI SI 09 - Change Management
xviii. POI SI 10 - Classificazione delle Informazioni
xix. POI SI 11 - Manutenzione delle apparecchiature
xx. POI SI 12 - Business impact analisys
xxi. POI SI 13 - Procedura per le comunicazioni
xxii. IDL SIA 07 - Piano di Disaster Recovery di risorse assegnate al Team AT
xxiii. IDL SIA 08 - Piano di Disaster Recovery di risorse assegnate al Team DR
xxiv. IDL SIA 09 - Piano di Disaster Recovery di risorse assegnate al Team ED
xxv. IDL SIA 10 Piano di Disaster Recovery di risorse assegnate al Team HR
xxvi. IDL SIA 11 Piano di Disaster Recovery di attività di parti interessate rilevanti

- ISO 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks

2. SCOPO

La presente politica indirizza le modalità con le quali PA Digitale S.p.A., in relazione alla propria missione, definisce ed attua i principi relativi alla identificazione e all'effettivo esercizio dei ruoli e delle responsabilità in materia di sicurezza delle informazioni tra la stessa PA Digitale e il provider di servizi cloud (di seguito denominato "Provider").
L'attuazione del modello di Responsabilità di Security Condivisa (SSRM – Shared Security Responsibility Model) presuppone:

- l'intervenuta scelta del cloud services provider (CSP) secondo le modalità e i criteri stabiliti dalla procedura POI ACQ 01 - Gestione fornitori e ordini di acquisto e relativi allegati
- l'identificazione della tipologia di servizio erogato dal CSP (IaaS o PaaS)

In linea di principio e per caratterizzazione generale, quando un atto normativo o regolamentare attribuisce specifiche responsabilità al cloud services provider, queste si intendono definite in via prioritaria come applicazione obbligatoria, anche in sostituzione di eventuali clausole contrarie difformi, secondo il principio dell'art. 1339 del codice civile.

In materia di articolazione della responsabilità per il trattamento dei dati, in riferimento all'art. 28 del Regolamento UE 2016/679 (GDPR), il fornitore di servizi cloud (CSP) è nominato responsabile (o sub-responsabile), con l'attribuzione delle istruzioni di trattamento derivanti dallo specifico accordo con il titolare in relazione alla natura e tipologia di servizio espletato.
La presente politica impegna PA Digitale nella definizione delle clausole contrattuali per i servizi cloud necessari all'erogazione dei propri servizi sia verso la pubblica Amministrazione che verso i privati.

3. RESPONSABILITÀ

Responsabile dell'attuazione della presente politica è l'Amministratore Delegato di PA Digitale che si avvale, per la verifica della corretta implementazione, del Responsabile della struttura Cybersecurity di Gruppo.

4. DEFINIZIONE DI RESPONSABILITÀ DI SECURITY CONDIVISA

L'identificazione delle responsabilità condivise nella dinamica dei servizi cloud dipende dalla tipologia di servizio acquisito. In particolare:

a) Per PaaS, il provider cloud gestisce l'infrastruttura informatica per la piattaforma ed esegue il software cloud che fornisce i componenti della piattaforma, come stack di esecuzione del software runtime, database e altri componenti middleware. Il fornitore di servizi cloud PaaS in genere supporta anche il processo di sviluppo, distribuzione e gestione del consumatore cloud PaaS fornendo strumenti quali ambienti di sviluppo integrati (IDE), versione di sviluppo del software cloud, kit di sviluppo software (SDK), strumenti di distribuzione e gestione. Il Consumatore PaaS Cloud ha il controllo sulle applicazioni ed eventualmente su alcune impostazioni dell'ambiente di hosting, ma non ha accesso o ha accesso limitato all'infrastruttura sottostante la piattaforma come rete, server, sistemi operativi (SO) o spazio di archiviazione.
b) Per IaaS, il Cloud Provider acquisisce le risorse informatiche fisiche alla base del servizio, inclusi server, reti, infrastrutture di storage e hosting. Il provider cloud esegue il software cloud necessario per rendere le risorse informatiche disponibili al consumatore cloud IaaS attraverso una serie di interfacce di servizio e astrazioni di risorse informatiche, come macchine virtuali e interfacce di rete virtuale. Il consumatore cloud IaaS a sua volta utilizza queste risorse informatiche, come un computer virtuale, per le sue esigenze informatiche fondamentali. Rispetto ai consumatori cloud SaaS e PaaS, un consumatore cloud IaaS ha accesso a forme più fondamentali di risorse informatiche e quindi ha un maggiore controllo sul più componenti software in uno stack di applicazioni, inclusi il sistema operativo e la rete. Il provider cloud IaaS, d'altro canto, ha il controllo sull'hardware fisico e sul software cloud che rendono possibile la fornitura di questi servizi infrastrutturali, ad esempio server fisici, apparecchiature di rete, dispositivi di archiviazione, sistema operativo host e hypervisor per la virtualizzazione.

La figura che segue descrive in linea astratta la suddivisione

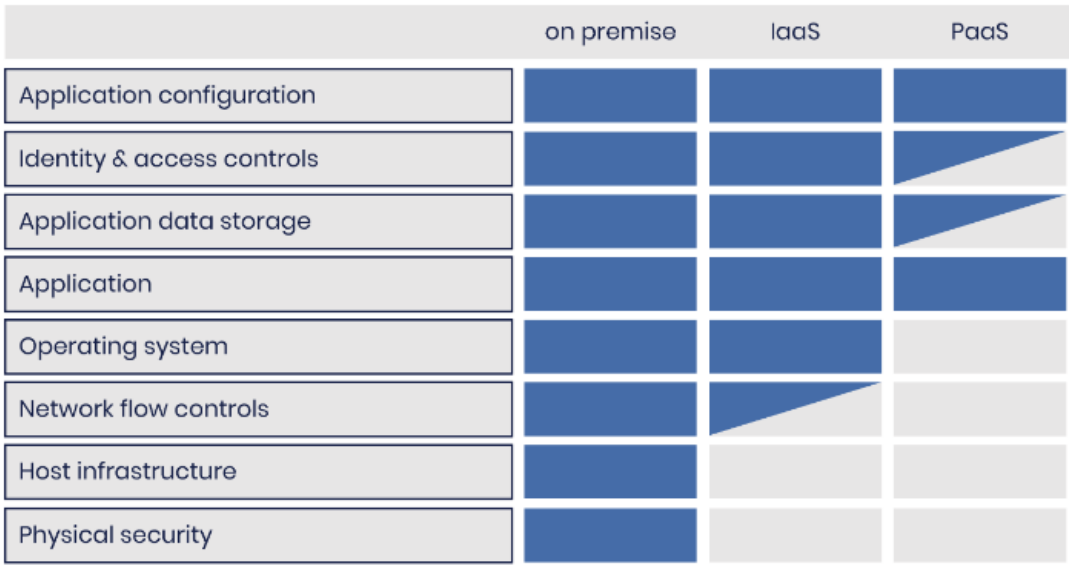

Fig. 1 – Modello astratto di responsabilità condivisa

LEGENDA:

la responsabilità di security è del soggetto che detiene la titolarità primaria dei dati

la responsabilità di security è condivisa tra consumatore cloud e provider

la responsabilità di security appartiene esclusivamente al provider

Il contratto di servizio che lega PA Digitale al Cloud Services Provider selezionato definisce:

a) In maniera univoca la tipologia di servizio acquisito (IaaS o PaaS)
b) I controlli normativi che appartengono all'area di responsabilità, desunti dal provvedimento dell'Agenzia per la Cybersicurezza Nazionale assunto con Determinazione n. 307 del 18 gennaio 2022, come modificate dal Decreto n. 20610 del 28 luglio 2023 e, per la componente di servizi critici, con riferimento al contenuto della Determina ACN n. 306 del 18 gennaio 2022 - "AGGIORNAMENTO DEGLI ULTERIORI LIVELLI MINIMI DI SICUREZZA, CAPACITÀ ELABORATIVA, E AFFIDABILITÀ DELLE INFRASTRUTTURE DIGITALI PER LA PUBBLICA AMMINISTRAZIONE E DELLE ULTERIORI CARATTERISTICHE DI QUALITÀ, SICUREZZA, PERFORMANCE E SCALABILITÀ DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE, NONCHÉ REQUISITI DI QUALIFICAZIONE DEI SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE" (articoli 7, 8, 11 del Regolamento di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, adottato dall'Agenzia per l'Italia digitale ai sensi dell'articolo 17, comma 6, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)
c) Gli specifici controlli, riferibili a standard correnti (ISO 27017, ISO 27018, ISO 27035 - con riguardo ai controlli ISO 27002 applicabili)

5. RESPONSABILITÀ DEL PROVIDER

Competono in via esclusiva al Cloud Services Provider, in particolare, i seguenti ambiti di responsabilità:

Dominio	Obiettivi	***Riferimento normativo/standard***
Organizzazione della sicurezza	Il fornitore di servizi cloud deve istituire, mantenere ed aggiornare, ottenendo le relative certificazioni da un ente di certificazione accreditato, un sistema di gestione della sicurezza, per il proprio ambito, con riguardo alle seguenti norme: a) una certificazione ISO 9001 - Sistemi di Gestione per la Qualità (SGQ) per l'infrastruttura digitale oggetto di qualifica; b) una certificazione ISO/IEC 27001:2022 - Sistema di gestione per la sicurezza delle Informazioni per l'infrastruttura digitale oggetto di qualifica, con estensione alle linee guida ISO 27017:2015, ISO 27018:2019 e ISO 27035:2015 c) una certificazione ISO 22301:2019 - Business Continuity-Management System (Gestione della continuità operativa) per l'infrastruttura digitale oggetto di qualifica). All'interno di tale ambito, il fornitore deve definire e dimostrare: a) La definizione di ruoli e responsabilità per la sicurezza b) La separazione dei ruoli (segregation of duties) c) La pianificazione attuazione e sviluppo della gestione del rischio d) La gestione degli incidenti di sicurezza e) La gestione delle vulnerabilità f) La gestione del cambiamento g) Le pratiche di continuo miglioramento	***ISO 27017 – CLD.6.3 (accordo sulle responsabilità condivise); D.Lgs. 138/2024, art. 21 (misure di gestione del rischio); ISO/IEC 27001:2022***
Responsabilità sulle risorse tecnologiche	Il Fornitore dei servizi cloud è esclusivo responsabile: a) Della pianificazione e gestione della disponibilità, qualità e adeguata capacità delle risorse per rispondere alle esigenze di disponibilità e continuità operativa definite da PA	***ISO 27017 – CLD.9.5 (sicurezza degli ambienti virtuali del provider); D.Lgs. 138/2024, art. 21, c. 2, lett. a) (sicurezza delle reti e dei***

	Digitale; b) delle risorse tecnologiche (server, sistemi di elaborazione e di storage; sistemi di network, sistemi di sicurezza ad esso afferenti e ogni elemento – incluse le tecnologie di servizio per garantire la continuità operativa come continuità dell'erogazione della rete elettrica, sistemi di raffreddamento HVAC, sistemi di prevenzione e spegnimento incendi; sistemi di prevenzione e contenimento alluvioni) che costituiscono l'elemento essenziale per l'erogazione dei propri servizi e ne è esclusivo titolare; c) del monitoraggio, cifratura, riservatezza delle comunicazioni tra ambienti per garantire che siano possibili soltanto comunicazioni autenticate e autorizzate; d) dell'hardening dei sistemi operativi host e guest, degli hypervisor e degli altri elementi infrastrutturali critici; e) definire, implementare e valutare processi tecnici di protezione approfondita per la protezione dell'ambiente cloud privato e/o multitenant pubblico; f) delle attività di monitoraggio, controllo e risposta ad atti di interferenza illecita posti in essere dal proprio personale; g) della effettiva e piena segregazione degli strumenti utilizzati per la garanzia di sicurezza e continuità delle operazioni, evitando p. es. potenziali rischi di commistione tra sistemi operativi e gestionali; tra sistemi di produzione e non produzione; trasmigrazione di codice malevolo da applicativi di posta elettronica agli ambienti di produzione o inappropriato utilizzo della navigazione internet è altresì cura esclusiva del Fornitore dei servizi cloud la gestione della propria catena delle forniture.	***sistemi); GV.SC-07 (ACN 379907/2025)***

Sicurezza delle risorse umane	Il Fornitore dei servizi cloud è esclusivo responsabile della selezione, del reclutamento, della formazione del personale adibito allo specifico servizio, inclusi gli obblighi intesi a prevenire il rischio di minacce interne; nonché alla specifica formazione tecnica e di sicurezza;	***ISO 27017 – CLD.6.3; D.Lgs. 138/2024, art. 21, c. 2, lett. g) (pratiche di igiene informatica e formazione); ISO/IEC 27001:2022, A.6***
Sicurezza fisica e ambientale	Il Fornitore dei servizi cloud è esclusivo responsabile del mantenimento dei livelli di sicurezza fisica ed ambientale, con particolare riguardo a: a) Idoneità strutturale e tecnologica degli immobili nei quali sono ospitate le tecnologie di servizio, anche riguardo a specifiche minacce fisiche antropiche e non antropiche b) Definizione delle regole e relativa attuazione per l'accesso fisico: o alle strutture in cui sono installati i sistemi informativi, gli storage e i sistemi complementari necessari al loro funzionamento (approdi di fibra, sistemi di trasformazione elettrica, gruppi elettrogeni e di continuità, unità di trattamento aria, sistemi di intercettazione carburanti, partizionatori elettrici, sistemi di prevenzione e spegnimento incendi; sistemi di prevenzione alluvioni e simili) o agli specifici componenti tecnologici, in relazione al ruolo di amministratori di sistemi o con elevati privilegi; c) gestione di processi relativi all'obsolescenza tecnologica e al ciclo di vita delle tecnologie e dei supporti di memorizzazione	***ISO 27017 – CLD.6.3; D.Lgs. 138/2024, art. 21, c. 2, lett. e) (sicurezza fisica e dell'ambiente); PR.IR-01 (ACN 379907/2025)***
Sicurezza e continuità delle comunicazioni	Il Fornitore dei servizi cloud è esclusivo responsabile della sicurezza e continuità delle comunicazioni, sin dalla fase della progettazione, intese come assicurazione della componente di networking interno (LAN operative interne al singolo centro di	***ISO 27017 – CLD.13.1.4 (allineamento delle politiche di sicurezza delle reti); D.Lgs. 138/2024, art. 21, c.***

	elaborazione o tra più centri, al fine di garantire i livelli di sicurezza e continuità attesa; in particolare l'effettiva funzionalità degli obiettivi di continuità operativa e, in particolare, la effettiva, reale e documentata funzionalità delle logiche di Disaster Recovery), sia riguardo alle reti pubbliche di propria pertinenza. In particolare, a titolo di esempio, il Fornitore dei servizi cloud risponde in via esclusiva: a) della segregazione interna delle reti, per garantire gli obiettivi di sicurezza attesi da possibili movimenti laterali tra componenti dei diversi tenant, con misure tecniche, organizzative e di processo dimostrabili; b) della funzionalità dei presidi di controllo per i processi di continuità operativa; c) della gestione delle connessioni tra le proprie infrastrutture e la rete pubblica, con particolare riguardo ai livelli di sicurezza richiesti verso i fornitori di servizi di connettività che permettono l'accesso alle risorse cloud. I relativi contratti di servizio devono poter garantire, almeno, gli stessi livelli di continuità di servizio stabiliti dalla normativa vigente e dal contratto	***2, lett. a) (sicurezza delle reti); PR.IR-01 (ACN 379907/2025)***
Gestione della continuità operativa delle infrastrutture	Il Fornitore dei servizi cloud è esclusivo responsabile nell'assicurare la continuità operativa delle proprie infrastrutture tecnologiche, per modo da assicurare, nel quadro delle obbligazioni normative e contrattuali, i livelli di servizio stabiliti. In particolare, spetta in via esclusiva di stabilire, documentare, approvare, comunicare, applicare, valutare e aggiornare un piano operativo di gestione degli eventi avversi, di qualunque natura, che possano costituire un impedimento all'esercizio operativo, per garantire l'obiettivo di continuità operativa stabilito da norme di legge o di contratto Tale obbligo si estende, in particolare; a) Alle capacità infrastrutturali per la funzionalità dei server a servizio di	***ISO 27017 – CLD.12.1.3 (gestione della capacità del provider); D.Lgs. 138/2024, art. 21, c. 2, lett. c) (continuità operativa e gestione delle crisi); ISO 22301:2019***

	macchine virtuali, hypervisor e sistemi complementari; b) Alle capacità di storage stabilite; c) Alle capacità di backup e restore. In particolare, è responsabilità non negoziabile la produzione di non meno di 3 copie di backup di cui almeno una fisicamente custodita in una posizione diversa dal luogo in cu sono ubicate le apparecchiature di trattamento dei dati di PA Digitale e comunque garantendo che le altre copie siano logicamente segregate, con le appropriate misure di sicurezza, dall'ambiente di produzione. È altresì responsabilità esclusiva del fornitore dei servizi cloud, quando contrattualizzato il servizio di backup ad alta affidabilità, che le routine di backup vengano effettuate con la periodicità stabilità assieme alle prove di integrità e ripristino; d) Alla verifica dell'effettività delle strategie di business continuity attraverso test, esercitazioni e verifiche, con documentazione resa disponibile.	
Sicurezza delle informazioni relativa ai sistemi e alle reti	Compete in via esclusiva al Fornitore dei servizi cloud la gestione della sicurezza delle informazioni della propria infrastruttura, inclusi, a titolo di esempio: a) L'attuazione dei principi di security by design della propria infrastruttura, per soddisfare i requisiti di legge e contrattuali; b) L'attuazione dei principi di security lungo il ciclo di vita della propria infrastruttura, per garantire il livello di sicurezza atteso da norme regolamentari e contrattuali c) I controlli relativi alla sicurezza delle reti, con particolare riguardo alla protezione esterna (firewalling, intrusion detection/intrusion protection) d) I controlli sugli accessi e relative operazioni anomale	***ISO 27017 – CLD.9.5; CLD.16.1.3 (responsabilità del provider nella gestione degli incidenti); D.Lgs. 138/2024, artt. 21 e 25 (misure di sicurezza e notifica incidenti); GV.SC-01 (ACN 379907/2025)***

	e) La prevenzione delle minacce e la gestione delle vulnerabilità, con particolare riguardo a quelle che hanno impatto sui sistemi di networking, di virtualizzazione, ai sistemi operativi e alle componenti sotto l'esclusivo dominio del fornitore dei servizi cloud; f) La gestione delle obsolescenze sul software operativo dell'infrastruttura; g) L'attuazione delle politiche di controllo accessi, incluso il provisioning e il deprovisioning delle abilitazioni del personale, con la rigida attuazione del principio dei privilegi minimi; h) L'efficace monitoraggio dell'intera infrastruttura, secondo le migliori pratiche internazionali generalmente riconosciute, oltre alle regole specifiche applicabili per effetto di disposizioni normative e regolamentari; i) L'esecuzione di penetration tests e vulnerability assessment sull'infrastruttura, con obbligo specifico di conferimento delle risultanze j) La raccolta, tenuta e analisi dei log dei sistemi k) La gestione della verifica operativa degli amministratori di sistema	

6. RESPONSABILITÀ DI PA DIGITALE

Competono in via esclusiva a PA Digitale:

Dominio	Obiettivi	***Riferimento normativo/standard***
Organizzazione della sicurezza	PA Digitale, quale utilizzatore cloud, è tenuta a istituire, mantenere e aggiornare, ottenendo le relative certificazioni da un ente di certificazione accreditato, un sistema di gestione della sicurezza, per il proprio ambito, in relazione alla gestione degli applicativi installati sull'infrastruttura del Fornitore Cloud	***ISO 27017 – CLD.6.3 (obblighi del cloud service customer); D.Lgs. 138/2024, art. 24 (misure di gestione del rischio del consumer); ISO/IEC 27001:2022***
Responsabilità	PA Digitale è esclusivo responsabile delle	***ISO 27017 – CLD.9.5***

sulle risorse	proprie risorse tecnologiche necessarie: a) alla gestione delle applicazioni e del corretto allineamento dei data base, ferma restando l'esclusiva titolarità dei dati in capo agli utenti finali; b) alla gestione degli accessi dei propri dipendenti e di altre persone abilitate con qualifica di amministratori di sistema; c) alla gestione degli accessi alle applicazioni dei propri utenti	***(gestione degli ambienti virtuali da parte del customer); D.Lgs. 138/2024, art. 24, c. 2; GV.SC-05 (ACN 379907/2025)***
Sicurezza delle risorse umane	PA Digitale è esclusiva responsabile della selezione, del reclutamento, della formazione del proprio personale adibito allo specifico servizio relativo alle applicazioni, inclusi gli obblighi intesi a prevenire il rischio di minacce interne; nonché alla specifica formazione tecnica e di sicurezza	***ISO 27017 – CLD.6.3; D.Lgs. 138/2024, art. 21, c. 2, lett. g) (formazione in materia di cybersicurezza); ISO/IEC 27001:2022, A.6***
Sicurezza delle informazioni relativa ai sistemi e alle reti	PA Digitale è responsabile in via esclusiva a implementare e mantenere policy di sicurezza per le applicazioni e i dati ospitati dal Provider, con riguardo: a) alla sicurezza delle proprie applicazioni secondo i principi dello sviluppo sicuro del codice e lungo il ciclo di vita; b) all'adempimento degli obblighi specificamente imposti da norme cogenti attribuite in via esclusiva al cloud consumer qualificato; c) alla corretta configurazione dei servizi cloud nella propria responsabilità; d) alla sicurezza delle infrastrutture e delle reti afferenti al proprio ambito operativo *on premises*; e) ai controlli sugli accessi alle applicazioni e relative operazioni anomale; f) alla regolamentazione della cifratura delle applicazioni, se non diversamente stabilito; g) alla prevenzione delle minacce e la gestione delle vulnerabilità delle applicazioni, nel perimetro di responsabilità del consumer cloud; h) alla gestione delle obsolescenze sul	***ISO 27017 – CLD.9.5; CLD.13.1.4; D.Lgs. 138/2024, artt. 24 e 29 (sicurezza applicazioni e catena di approvvigionamento); PR.DS-01/PR.DS-02 (ACN 379907/2025)***

	software applicativo; i) all'attuazione delle politiche di controllo accessi sulle applicazioni, incluso il provisioning e il deprovisioning delle abilitazioni del personale, con la rigida attuazione del principio dei privilegi minimi; j) al monitoraggio di sicurezza del front-end applicativo	

7. COOPERAZIONE E COMPLIANCE

Entrambe le parti devono collaborare per garantire la conformità alle leggi e normative applicabili sulla protezione dei dati, inclusa la GDPR ove applicabile. In particolare, competono al Fornitore dei servizi Cloud tutti gli obblighi di dimostrazione di conformità relativi a norme cogenti e gli obblighi di certificazione previsti da norme di contratto o di regolamento amministrativo ovvero da norme di legge.

7.1 Gestione del rischio

La gestione del rischio, nella specificità delle responsabilità, è una gestione condivisa e devono essere attuate idonee misure per lo scambio attivo e tempestivo di elementi, per permettere a ciascuna delle Parti di identificare, valutare e controllare i rischi che attengono ai rispettivi ambienti e permettere la reciproca azione di continuo miglioramento.

7.2 Adempimenti specifici in materia di dati personali

Il trattamento dei dati è disciplinato dal Regolamento UE 2026/679 (GDPR). La materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di Dati Personali, le categorie di interessati e le obbligazioni e i diritti di PA Digitale sono stabiliti nel contratto.
In linea generale, il Fornitore di servizi Cloud dovrà:

a) trattare i Dati Personali soltanto su istruzione documentata della Società, con esclusione di trattamenti in Paesi diversi dell'Unione Europea;
b) garantire che le persone autorizzate al trattamento dei Dati Personali si siano impegnate alla riservatezza o abbiano un'adeguata obbligazione legale di riservatezza;
c) adottare tutte le misure richieste ai sensi dell'Articolo 32 del Regolamento Generale sulla Protezione dei Dati;
d) rispettare le condizioni di cui ai paragrafi 1 e 3 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assistere la Società con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligazione di PA Digitale di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del Regolamento Generale sulla Protezione dei Dati;

f) assistere PA Digitale nel garantire il rispetto delle obbligazioni di cui agli Articoli da 32 a 36 del Regolamento Generale sulla Protezione dei Dati, tenendo conto della natura del trattamento e delle informazioni messe a disposizione del Fornitore di servizi cloud;
g) PA Digitale si riserva la facoltà di impartire disposizioni di eliminare o restituire tutti i Dati Personali dopo che è terminata l'erogazione dei servizi relativi al trattamento ed eliminare le copie esistenti (con modalità di cancellazione sicura), salvo che il diritto dell'Unione o degli Stati Membri preveda la conservazione dei dati;
h) mettere a disposizione di PA Digitale tutte le informazioni necessarie per dimostrare il rispetto delle obbligazioni stabilite all'Articolo 28 del GDPR e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate da PA Digitale o da un altro soggetto da questa incaricato.

7.3 Sistemi crittografici

Il fornitore dei servizi cloud permette l'esecuzione sulla propria piattaforma delle attività crittografiche, in particolare di cifratura dei dati. Nella definizione delle attività contrattuali, le Parti stabiliscono a chi competa il processo di cifratura e la relativa modalità di gestione, assegnando i relativi ruoli e responsabilità.

8. GESTIONE DEGLI INCIDENTI E ATTIVITÀ FORENSI

Ferme restando le rispettive responsabilità esclusive in capo al Fornitore dei servizi Cloud e PA Digitale, deve essere condiviso un piano di gestione degli incidenti che tenga conto delle seguenti necessità:

a) Tempestività dell'informazione: il fornitore dei servizi cloud è tenuto a notificare ogni evento che abbia impatto o possa avere impatto sulla disponibilità, integrità e riservatezza delle informazioni, dei dati o dei servizi informatici: immediatamente e senza ritardo, se bloccanti il servizio; altrimenti entro 3 (tre) ore. Rientrano negli eventi oggetto di segnalazione sia gli atti umani deliberati e volontari, sia gli eventi umani involontari o negligenti, nonché gli eventi naturali, inclusi quelli di causa ignota o di avaria tecnica. Per quanto attiene alla tassonomia, c si riferisce alle tabelle di cui all'Allegato A del Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81;
b) Completezza dell'informazione: il Fornitore dei servizi cloud fornisce ogni utile dettaglio a PA Digitale, sulla natura dell'evento, sulla valutazione iniziale e perdurante delle cause e degli impatti e qualunque altro elemento utile a definire lo scenario e le possibili evoluzioni;
c) La responsabilità della gestione dell'incidente è condivisa e deve essere definito un piano di risposta agli incidenti che chiarisca le responsabilità di entrambe le parti in caso di violazione della sicurezza, le azioni da intraprendere per il contenimento degli effetti dell'incidente e il ripristino.

9. RESPONSABILITÀ DEI CLIENTI/UTILIZZATORI FINALI DEI SERVIZI EROGATI DA PA DIGITALE S.P.A.

La presente sezione disciplina il ruolo di PA Digitale S.p.A. quale fornitore di prodotti e servizi in modalità SaaS (Software as a Service) nei confronti dei propri Clienti e definisce le responsabilità che tali Clienti assumono in qualità di "Utilizzatori Finali" dei Servizi erogati da PA Digitale.

9.1 Ambito di applicazione e quadro normativo di riferimento

La presente sezione è governata, in via cumulativa e senza deroghe, dalle seguenti fonti normative e standardistiche già richiamate al capitolo 1 della presente Politica. Nella catena di fornitura cloud, PA Digitale si configura contestualmente come:

a) cloud consumer nei confronti del proprio Cloud Services Provider (CSP), secondo quanto disciplinato ai capitoli precedenti della presente Politica SSRM;

b) cloud service provider SaaS nei confronti dei propri Clienti, ai quali eroga i Servizi mediante il proprio Internet Data Center (IDC) qualificato ACN. In tale veste, PA Digitale assume il ruolo di cloud service provider (CSP) ai sensi della ISO/IEC 27017:2015, con le relative responsabilità di controllo.

9.2 Responsabilità di PA Digitale come fornitore SaaS

In qualità di cloud service provider SaaS, PA Digitale è esclusiva responsabile dei seguenti ambiti. Per ciascun dominio è indicato il controllo ISO/IEC 27017:2015 e/o la misura NIS2/decreto NIS applicabile, desunti dai riferimenti già citati al capitolo 1 e al capitolo 4 della presente Politica.

Dominio	*Obiettivi e obblighi di PA Digitale*	*Riferimento normativo/standard*
Erogazione del Servizio e continuità	***PA Digitale garantisce l'erogazione dei Servizi SaaS, mediante la propria organizzazione, risorse qualificate e infrastruttura IDC qualificata ACN. È responsabile della gestione della continuità operativa dei propri applicativi verso i Clienti.***	***ISO 27017 – CLD.6.3; D.Lgs. 138/2024, art. 24***
Sicurezza dell'infrastruttura applicativa	***PA Digitale è responsabile della sicurezza dei propri applicativi secondo i principi di sviluppo sicuro del codice lungo l'intero ciclo di vita del software; della corretta configurazione dei***	***ISO 27017 – CLD.9.5; CLD.12.1.3; PR.IR-01 (ACN 379907/2025)***

Dominio	*Obiettivi e obblighi di PA Digitale*	*Riferimento normativo/standard*
	servizi cloud nella propria responsabilità; della gestione delle vulnerabilità applicative; del monitoraggio di sicurezza del front-end applicativo.	
Gestione delle credenziali di accesso	***PA Digitale è responsabile del processo di generazione, rilascio, sospensione e rigenerazione delle credenziali di primo accesso (User ID e Password) attribuite ai Clienti per la fornitura e l'attivazione dei Servizi.***	***ISO 27017 – CLD.9.5; CLD.6.3***
Riservatezza e protezione dei dati	***PA Digitale assicura la segretezza e la confidenzialità dei dati del Cliente. I servizi SaaS si basano su un IDC localizzato fisicamente in Italia. Nessun dato personale viene elaborato per scopi indipendenti dalle istruzioni del Cliente. PA Digitale assume, ove nominata, il ruolo di Responsabile esterno del trattamento ai sensi dell'art. 28 GDPR.***	***ISO 27017 – CLD.13.1.4; PR.DS-01/PR.DS-02 (ACN 379907/2025); GDPR, art. 28***
Portabilità e restituzione dei dati	***In caso di cessazione del contratto, PA Digitale garantisce al Cliente la disponibilità dei propri dati per un periodo definito contrattualmente, con possibilità di esportazione mediante dump files in formato aperto e interoperabile. Decorso tale termine, i dati vengono cancellati con modalità sicura.***	***ISO 27017 – CLD.8.1.5; D.Lgs. 138/2024, art. 24, c. 2***
Gestione e notifica degli incidenti	***PA Digitale notifica tempestivamente al Cliente ogni evento che abbia impatto o possa avere impatto sulla disponibilità, integrità e riservatezza dei dati e dei servizi, secondo le tempistiche***	***ISO 27017 – CLD.16.1.3; D.Lgs. 138/2024, art. 25; ACN Det. 379907/2025, All. 4***

Dominio	*Obiettivi e obblighi di PA Digitale*	*Riferimento normativo/standard*
	previste dalla normativa vigente. In qualità di soggetto essenziale, PA Digitale ottempera agli obblighi di notifica all'ACN: pre-notifica entro 24 ore, notifica completa entro 72 ore, relazione finale entro un mese, ai sensi dell'art. 25 del decreto NIS. I criteri di classificazione applicabili sono quelli dell'Allegato 4 della Determinazione ACN n. 379907/2025 (codici IS-1, IS-2, IS-3, IS-4).	

9.3 Obblighi e responsabilità del Cliente utilizzatore dei Servizi SaaS di PA Digitale

Il Cliente, in qualità di utilizzatore finale dei Servizi SaaS erogati da PA Digitale, assume in via esclusiva i seguenti obblighi e responsabilità. Ai sensi della ISO/IEC 27017:2015, il Cliente riveste il ruolo di cloud service customer (CSC) e gli competono i controlli specificamente attribuiti a tale soggetto dallo standard.

	Obbligo	*Contenuto*	*Riferimento normativo/standard*
a)	***Utilizzo corretto dei Servizi***	***Il Cliente è tenuto a utilizzare i Servizi conformemente alle istruzioni ricevute da PA Digitale e nel rispetto dei prerequisiti hardware e software stabiliti. Il non corretto utilizzo dei Servizi o dell'ambiente SaaS da parte del proprio personale esonera PA Digitale da ogni responsabilità per i disservizi che ne derivino.***	***ISO 27017 – CLD.6.3; D.Lgs. 138/2024, art. 24***
b)	***Custodia e gestione delle credenziali***	***Il Cliente è esclusivo responsabile della custodia e del corretto utilizzo delle***	***ISO 27017 – CLD.9.5; GV.SC-05 (ACN 379907/2025)***

	Obbligo	***Contenuto***	***Riferimento normativo/standard***
		proprie credenziali di autenticazione e accesso, nonché di ogni conseguenza dannosa derivante dal loro smarrimento, sottrazione o compromissione. Le credenziali possono essere comunicate esclusivamente ai propri incaricati che debbano utilizzare i Servizi nell'esercizio delle loro mansioni. È fatto assoluto divieto di cedere i Servizi a terzi o di consentire l'accesso a soggetti non autorizzati.	
c)	***Titolarità dei dati e conformità normativa***	***Il Cliente mantiene la piena titolarità delle informazioni immesse attraverso gli applicativi fruiti in modalità SaaS e assume ogni responsabilità civile e penale in ordine al loro contenuto. Il Cliente è altresì tenuto a conoscere le disposizioni di legge vigenti con riferimento alla materia elaborata dagli applicativi e a controllare l'esattezza dei risultati ottenuti.***	***ISO 27017 – CLD.8.1.5; D.Lgs. 138/2024, art. 24, c. 2***
d)	***Protezione dei dati personali – Titolare del trattamento***	***Il Cliente opera quale Titolare del trattamento ai sensi del GDPR (Reg. UE 2016/679). È tenuto a operare e vigilare affinché l'attività dei propri incaricati venga svolta nel rispetto delle disposizioni legislative in materia di protezione dei dati personali e a nominare PA***	***GDPR, artt. 24 e 28; ISO 27017 – CLD.13.1.4; PR.DS-01/PR.DS-02 (ACN 379907/2025)***

	Obbligo	*Contenuto*	*Riferimento normativo/standard*
		Digitale Responsabile esterno del trattamento, con le istruzioni documentate richieste dall'art. 28 GDPR.	
e)	***Sicurezza dell'ambiente del Cliente***	***Nel proprio ambiente, il Cliente è tenuto ad adottare ogni cautela necessaria alla protezione dei dati mediante specifici e aggiornati programmi antivirus; ad attuare sistemi di sicurezza logici, fisici e organizzativi idonei a impedire l'accidentale o incontrollata consultazione, esportazione, lettura, copiatura, distruzione, comunicazione o diffusione dei dati trattati nell'esecuzione del contratto, nel rispetto delle misure di sicurezza di cui al GDPR (art. 32).***	***ISO 27017 – CLD.9.5; GDPR, art. 32; PR.IR-01 (ACN 379907/2025)***
f)	***Segnalazione degli incidenti di sicurezza***	***Il Cliente è tenuto a comunicare tempestivamente a PA Digitale qualsiasi alterazione ai parametri di sicurezza del servizio o qualsiasi evento che possa avere impatto sulla disponibilità, integrità e riservatezza dei dati. Le violazioni dei dati personali ai sensi degli artt. 33–34 GDPR restano in capo al Cliente quale Titolare del trattamento. La notifica all'ACN degli incidenti significativi, ove il Cliente sia a sua volta soggetto NIS2, rimane a esclusivo***	***ISO 27017 – CLD.16.1.3; D.Lgs. 138/2024, art. 25; GDPR, artt. 33–34***

	Obbligo	*Contenuto*	*Riferimento normativo/standard*
		carico del Cliente medesimo.	
g)	***Catena di approvvigionamento e sicurezza dei propri fornitori***	***Il Cliente è responsabile della sicurezza della propria catena di approvvigionamento IT e di garantire che i propri fornitori e subfornitori rispettino requisiti di sicurezza equivalenti a quelli stabiliti dalla normativa applicabile, in particolare laddove il Cliente sia a sua volta soggetto essenziale o importante ai sensi del decreto NIS.***	***ISO 27017 – CLD.6.3; GV.SC-01/GV.SC-07 (ACN 379907/2025); D.Lgs. 138/2024, art. 29***

9.4 Limitazione della responsabilità di PA Digitale verso i Clienti

Salvo i casi di dolo o colpa grave, PA Digitale non sarà in alcun caso responsabile per danni diretti e indiretti di qualsiasi natura che il Cliente, o terzi, possano subire in relazione all'uso o al mancato uso dei Servizi SaaS forniti, nei casi riconducibili a:

a) non corretto utilizzo dei Servizi SaaS o dell'ambiente SaaS da parte del personale del Cliente (ISO 27017 – CLD.6.3);

b) errori od omissioni del Cliente nel trasferimento dei dati a PA Digitale, o malfunzionamento di software o configurazioni hardware imputabili al Cliente;

c) inosservanze, inadempimenti e violazioni di legge imputabili al Cliente, incluse quelle in materia di protezione dei dati personali (GDPR) e di cybersicurezza (decreto NIS, D.Lgs. 138/2024);

d) sospensione del Servizio causata dai fornitori di PA Digitale (cloud provider upstream), nei limiti e con le esclusioni di responsabilità stabilite dal contratto di servizio cloud.

9.5 Raccordo con la supply chain

Le responsabilità degli utilizzatori finali descritte nel presente capitolo integrano e specificano, per il livello di fornitura SaaS verso i Clienti, il modello di responsabilità condivisa illustrato nei precedenti capitoli della presente Politica SSRM. La catena di responsabilità cloud (CSP → PA Digitale → Cliente) garantisce la coerenza e la tracciabilità delle responsabilità di sicurezza a tutti i

livelli della filiera, in conformità ai principi della ISO/IEC 27017:2015 (controllo CLD.6.3 – accordo sulle responsabilità condivise) e agli obblighi della catena di approvvigionamento di cui agli artt. 24 e 29 del D.Lgs. 138/2024 (decreto NIS).

10. MODIFICHE ALLA POLITICA

La presente politica può essere aggiornata o modificata in base all'evoluzione delle minacce alla sicurezza, alle modifiche apportate nei servizi cloud o alle nuove normative di legge e di regolamento applicabili.

11. AGGIORNAMENTO DEL QUADRO NORMATIVO NIS – RECEPIMENTO DELLA DIRETTIVA (UE) 2022/2555

I riferimenti alla Direttiva (UE) 2016/1148 (NIS1) e al Decreto legislativo 18 maggio 2018, n. 65, contenuti nella presente Politica SSRM, devono intendersi aggiornati rispettivamente alla Direttiva (UE) 2022/2555 (NIS2) e al Decreto legislativo 4 settembre 2024, n. 138 (decreto NIS), che li hanno abrogati con decorrenza 16 ottobre 2024, ai sensi dell'art. 41 del medesimo decreto.
PA Digitale S.p.A., in qualità di soggetto essenziale ai sensi dell'art. 6 del decreto NIS, ha adottato le misure di sicurezza di base di cui all'Allegato 2 della Determinazione ACN n. 379907 del 19 dicembre 2025, con specifico riferimento alle misure applicabili al modello di responsabilità condivisa con i fornitori di servizi cloud. Le misure adottate includono, per quanto rilevante ai fini del presente documento: GV.SC-01 e GV.SC-05 (requisiti di sicurezza nella catena di approvvigionamento, con obblighi contrattuali verso i provider cloud), GV.SC-07 (valutazione e monitoraggio del rischio dei fornitori), PR.IR-01 (protezione delle reti e degli ambienti da accessi non autorizzati), PR.DS-01 e PR.DS-02 (protezione dei dati a riposo e in transito).
Gli obblighi di notifica degli incidenti significativi di cui all'art. 25 del decreto NIS – ivi inclusa la pre-notifica entro 24 ore, la notifica completa entro 72 ore e la relazione finale entro un mese dalla consapevolezza dell'incidente – si applicano integralmente a PA Digitale S.p.A. con decorrenza gennaio 2026 (nove mesi dalla comunicazione di inserimento nell'elenco NIS). I criteri di classificazione degli incidenti significativi applicabili sono quelli di cui all'Allegato 4 della Determinazione ACN n. 379907/2025 (codici IS-1, IS-2, IS-3, IS-4). La presente Politica SSRM è aggiornata in sede di revisione periodica per recepire le eventuali prescrizioni specifiche che ACN potrà emettere ai sensi dell'art. 31 del decreto NIS.