

## CYBER SECURITY REQUISITI DI SICUREZZA

### INTRODUZIONE

Questo documento rappresenta un riepilogo delle principali normative applicabili e delle misure preventive adottate da A2A per garantire la sicurezza delle informazioni e delle risorse tecnologiche informatiche del Gruppo. Queste prescrizioni si applicano ai fornitori e alle Terze Parti che svolgono attività per conto di A2A.

Quanto di seguito riportato definisce gli obiettivi di sicurezza, lasciando alla documentazione di dettaglio eventualmente prodotta o disponibile allo startup o durante il progetto, la scelta dei meccanismi di sicurezza da implementare/integrare in considerazione anche del grado d'interconnessione dei sistemi e della tipologia d'informazioni scambiate.

I fornitori e le Terze Parti sono tenuti a rispettare:

- I requisiti delle **NORMATIVE COGENTI**;
- Gli **STANDARD INTERNAZIONALI (REGOLAMENTI APPLICABILI)**;
- Le **Condizioni Generali di Sicurezza e, ove applicabile, anche le Condizioni Specifiche di Sicurezza riportate nel presente documento**, le quali riassumo i **requisiti, le politiche e le procedure per la sicurezza** delle informazioni e delle risorse tecnologiche e informatiche di A2A.

## Condizioni di sicurezza generali

---

**Il Fornitore assicura il rispetto delle condizioni di sicurezza di seguito definite, impegnandosi ad integrarle ulteriormente sulla base di una valutazione complessiva di rischio effettuata dallo stesso secondo le circostanze, il tipo di prestazione specifica da eseguire nonché il tipo di dati eventualmente trattati nell'oggetto della prestazione. In particolare:**

- 1.1 dà atto di avere stabilito e adottato le misure e/o gli accorgimenti necessari e/o opportuni applicabili al servizio effettivamente svolto in ossequio alle norme vigenti e nel rispetto dei requisiti di sicurezza riportati nel presente documento, e anche superiori, per la mitigazione di ogni rischio ragionevolmente prevedibile di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati e/o sistemi con potenziali conseguenze sulla riservatezza, l'integrità e la disponibilità dei dati, delle risorse e dei servizi della Committente, di cui viene a conoscenza e a contatto durante lo svolgimento della propria attività.
- 1.2 ha identificato e designato una figura di contatto per le tematiche di security. Se richiesto fornisce alla Committente gli estremi della persona e/o della struttura designata.
- 1.3 garantisce che tutti i propri collaboratori, subappaltatori, subcontraenti e/o altri ausiliari, ove previsti, e Terzi comunque denominati coinvolti nell'erogazione dei servizi abbiano sottoscritto opportuni accordi di riservatezza, sono stati adeguatamente informati circa le proprie responsabilità in materia di sicurezza informatica e circa le misure da adottare descritte nel presente documento e/o messe a disposizione in futuro dalla Committente. Nel caso in cui il servizio venga svolto al di fuori dell'Unione Europea e/o il suo personale operi al di fuori del territorio dell'Unione Europea, lo stesso deve assicurare il rispetto degli adempimenti previsti dai Privacy Agreement (DPA) della Committente.
- 1.4 coinvolge il personale strettamente necessario all'erogazione dei servizi, assicurandone un'adeguata selezione in termini di competenze, esperienze ed affidabilità e garantendo che lo stesso sia debitamente formato sulle proprie responsabilità e sulle policy di sicurezza definite dal Fornitore. A tal proposito il Fornitore è tenuto mantenere sempre riservate tutte le informazioni scambiate durante lo svolgimento delle attività, così come quelle assunte in fase selettiva, o durante l'acquisto di beni, e fatta salva l'esplicita autorizzazione rilasciata in forma scritta dal Committente, al Fornitore è vietato cedere, consegnare, rendere disponibili a qualsiasi titolo, o comunque comunicare o divulgare per qualsiasi motivo e in qualsiasi momento il contenuto di tali informazioni a terzi, salvo i casi previsti per legge. A tal proposito è fatto divieto, per lo scambio di informazioni della

Committente con Terzi comunque denominati, dell'uso di repository o spazi di memoria di massa presenti ed offerti dalla rete Internet presso operatori di rete terzi (e.g., Dropbox; Google document ecc.).

- 1.5 si impegna a far sì che il proprio personale abbia un accesso limitato alle informazioni della Committente, esclusivamente per lo svolgimento delle prestazioni oggetto di contratto nel rispetto delle mansioni svolte e verifica con cadenza periodica la sussistenza delle condizioni per la conservazione delle autorizzazioni di accesso a tali informazioni (es. cambio di mansione). A tal proposito riconosce in qualsiasi momento alla Committente la facoltà di revocare l'autorizzazione per l'accesso ai propri asset e ad effettuare qualunque attività sui dati della Committente;
- 1.6 esegue verifiche al proprio interno e verso Terzi comunque denominati coinvolti nell'erogazione dei servizi, con cadenza periodica o in caso di cambiamenti significativi delle normative vigenti ed applicabili, sull'efficacia delle misure di sicurezza adottate impegnandosi a fornire su richiesta della Committente, previo congruo preavviso, evidenze a dimostrazione dell'effettiva verifica svolta con l'indicazione di eventuali aree di miglioramento individuate; Il fornitore inoltre contribuisce ad eventuali valutazioni del livello di adeguatezza complessivo della sicurezza portate avanti dalla Committente, per le parti di competenze oggetto del Contratto, riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e dei sistemi gestiti e/o realizzati sotto la propria responsabilità.
- 1.7 mette in atto tutte le iniziative necessarie secondo un operatore diligente del settore per intercettare, contenere e segnalare prontamente ad A2A, e in particolare al Cyber Security Operation Center della Committente attraverso l'indirizzo [iris@a2a.it](mailto:iris@a2a.it), eventuali violazioni, azioni anomale e/o attacchi informatici, che lo riguardano direttamente anche attraverso il proprio personale, e collabora, per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, fornendo reportistica sugli incidenti rilevati che potrebbe intaccare la riservatezza, confidenzialità, disponibilità dei dati e/o dei sistemi della Committente. A tal proposito il Fornitore ha definito processi e strumenti finalizzati a identificare e gestire eventi anomali in termini di sicurezza e garantisce che il suo personale e tutti i suoi collaboratori - inclusi Terzi comunque denominati coinvolti nell'erogazione dei servizi - siano a conoscenza del proprio ruolo e delle operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente.
- 1.8 consente alla Committente di verificare, previa comunicazione da inviarsi con congruo preavviso di dieci giorni lavorativi, attraverso attività di assessment e audit, l'efficacia delle misure di sicurezza tecniche e/o organizzative adottate, nonché la conformità del proprio operato rispetto al presente documento e/o ad eventuali ulteriori procedure comunicate dalla Committente in tema di sicurezza. L'attività di verifica riguarderà ambiti attinenti al servizio svolto. A tal proposito il Fornitore assicura la necessaria disponibilità e assistenza per fornire informazioni ed elementi utili all'attività di verifica, nel rispetto dei principi di riservatezza definiti al suo interno e si impegna a mettere a disposizione risorse adeguate per provvedere ad implementare nei tempi stabiliti di concerto con la Committente, senza oneri

aggiuntivi, eventuali raccomandazioni e/o suggerimenti concordati tra le parti per la risoluzione di gap e vulnerabilità di severità alta e critica, emergenti da tali verifiche.

- 1.9 si impegna a garantire la disponibilità del proprio servizio offerto nel rispetto delle procedure di continuità operativa condivise dalla Committente o messe a disposizione su richiesta e a restituire gli asset della Committente (compresi dati, licenze e apparati) senza ingiustificato ritardo e senza ostacolare la Committente qualora la stessa decida di rivolgersi a un altro fornitore, così da garantire la continuità del servizio.
- 1.10 nel caso in cui nell'oggetto della prestazione rientrano anche ambiti di fornitura tramite i quali sono erogati, per conto della Committente, servizi digitali di pubbliche amministrazioni e attraverso cui pertanto sono trattati dati di queste ultime, il fornitore garantisce il rispetto delle caratteristiche di qualità, sicurezza, performance, scalabilità, interoperabilità e portabilità ai sensi del Regolamento per la Pubblica Amministrazione adottato dall'AGID con Determinazione 628/2021 in esecuzione dell'art. 33-septies del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221.

## Condizioni di sicurezza specifiche

---

Ove applicabili, nel caso in cui per l'esecuzione delle prestazioni oggetto del Contratto sono previste attività di assistenza e/o configurazione e/o manutenzione correttiva/evolutiva e/o sviluppo/implementazione su risorse tecnologiche informatiche IT, OT e di sicurezza della Committente, il Fornitore, ove applicabile per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, assicura il rispetto delle condizioni di sicurezza specifiche di seguito definite, impegnandosi ad integrarle ulteriormente sulla base di una valutazione complessiva di rischio effettuata dalla Committente. In particolare:

- 1.11.1 adotta un modello di governance per la selezione e designazione del personale che opera sugli asset e risorse della Committente redigendo e aggiornando un elenco contenente gli estremi identificativi da poter mettere a disposizione della stessa su richiesta. In particolare, effettua una valutazione sull'esperienza, sulla capacità e sull'affidabilità delle figure professionali e comunica senza indebito ritardo alla Committente eventuali situazioni che potrebbero comportare la necessità di revocare autorizzazioni di accesso del proprio personale agli asset e risorse oggetto del presente contratto.
- 1.11.2 garantisce di aver posto in essere e di continuare a porre in essere tutte le azioni necessarie un corretto provisioning/deprovisioning di tutto il personale del Fornitore nel rispetto delle procedure di abilitazione, modifica e revoca degli accessi logici agli asset e risorse della Committente.
- 1.11.3 in relazione all'accesso logico, accetta il tracciamento e monitoraggio dei log parte della Committente finalizzato a garantire adeguati controlli di sicurezza per le operazioni svolte su asset e risorse della stessa.
- 1.11.4 per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, adotta misure di sicurezza anche organizzative per far sì che:
  - le credenziali ricevute dal proprio personale vengano correttamente custodite esclusivamente dalla figura professionale identificata al fine di evitare l'accesso a tali informazioni da parte di soggetti non formalmente autorizzati;
  - gli accessi agli asset e risorse della Committente oggetto del presente contratto avvengano unicamente attraverso i canali e gli strumenti e messi a disposizione dalla stessa (es. Virtual Private Network per accessi remoti, accesso con doppio fattore ove ritenuto necessario, ecc.) al fine di garantire che anche eventuali dispositivi utilizzati dal Fornitore siano preventivamente identificati e accedano alle sole risorse per cui sono autorizzati;
  - lo svolgimento delle attività in qualità di utenti privilegiati sui sistemi della Committente avvenga esclusivamente nel rispetto della normativa di riferimento e

sulla base delle procedure definite dalla Committente, tra cui accesso tramite piattaforma di mediazione e tracciamento delle attività privilegiate, nonché meccanismi di autenticazione a più fattori e in generale nel rispetto delle indicazioni definite in appositi documenti operativi predisposti dalla Committente.

- 1.11.5 garantisce che tutti i dispositivi utilizzati dal proprio personale per le prestazioni oggetto del contratto (es. pc fissi e portatili) siano sempre aggiornati, mantenuti e ben configurati, a perfetta regola d'arte, condizioni necessarie per poter accedere agli asset e risorse della stessa. In particolare, i dispositivi prevedono quanto meno:
- autenticazione basata su codice di identificazione unico e personale ("User ID") e credenziali ("password") segrete con configurazioni specifiche riguardanti lunghezza, complessità, storicità e durata nel rispetto dei principali standard, utilizzata e conservata esclusivamente dal soggetto a cui è affidata la postazione;
  - chiusura automatica delle sessioni utente interattive dopo un intervallo di tempo configurato;
  - dotazione di un software antivirus/anti-malware sempre aggiornato all'ultima versione disponibile, non disattivabile dall'utente;
  - sistemi firewall e antintrusione per il controllo e il rilevamento di connessioni e accessi non autorizzati (es. firewall del pc abilitato);
  - meccanismi/software attivi per la cifratura del disco dati;
  - aggiornamento automatico o manuale, del sistema operativo alle ultime versioni.
- 1.11.6 garantisce per tutti i dispositivi utilizzati dal proprio personale di aver posto in essere e di continuare a porre in essere tutti i meccanismi di controllo dell'integrità dei dati necessari e/o opportuni a verificare l'autenticità di software, firmware e informazioni gestite.
- 1.11.7 si attiene al rispetto dei principi di security by design garantendo la segregazione dei ruoli/funzioni nell'erogazione del servizio di assistenza e/o configurazione e/o manutenzione correttiva/evolutiva e/o sviluppo prevedano i dovuti passaggi in un ambiente di test prima dell'effettivo rilascio nell'ambiente operativo. In caso di intervento su asset e risorse che trattano dati della Committente, i test preliminari non dovranno utilizzare dati reali. L'eventuale utilizzo di dati reali, in assenza di un'alternativa ragionevole, preventivamente autorizzato dalla Committente deve essere limitato in termini di quantità di dati e tempistiche di utilizzo degli stessi nella misura minima necessaria allo svolgimento delle attività di test, a seguito dei quali dovranno essere cancellati. Su tali dati dovranno essere garantite misure di sicurezza corrispondenti a quelle previste negli ambienti produttivi.
- 1.11.8 per lo svolgimento di attività di configurazione e/o manutenzione correttiva/evolutiva e/o sviluppo, garantisce il rispetto dei principi di Secure Software Development Lifecycle previsti dai principali standard e best practice di settore (es. OWASP) nonché il rispetto di eventuali procedure e linea guida condivise dalla Committente o messe a disposizione dalla stessa su richiesta.

- 1.11.9 si attiene e contribuisce in maniera attenta alla tracciatura accurata delle operazioni di competenza all'interno degli strumenti e sulla base delle procedure condivise dalla Committente o messe a disposizione della stessa su richiesta (es. strumenti di ticketing).
- 1.11.10 esegue con regolarità riesami di sicurezza (es. Vulnerability Assessment/Penetration Test) sulle proprie infrastrutture e sugli asset utilizzati per l'erogazione del servizio al fine di rilevare vulnerabilità e/o falle e di risolvere tali vulnerabilità e i difetti attraverso l'installazione di specifiche patch o con tempestivi interventi di remediation. Ove prevista la messa a disposizione di componenti tecnologiche (es. server, periferiche, apparati di comunicazione, software e applicativi custom ecc.) da parte del Fornitore, lo stesso esegue controlli atti a identificare e documentare vulnerabilità di tali componenti prima della messa in esercizio, assicurando che le stesse siano aggiornate (a livello di firmware e patch di sicurezza) anche in conformità con i piani di manutenzione e supporto definiti dai produttori, e si impegna nel corso dell'esercizio per le parti di propria competenza a fornire e installare d'accordo con la Committente, e senza oneri aggiuntivi, tutte le patch di sicurezza necessarie per garantire una tempestiva capacità di risposta all'evoluzione delle minacce e delle vulnerabilità informatiche.
- 1.11.11 si adopera per intercettare attraverso presidi e processi di controllo e monitoraggio, incidenti/anomalie, intesi come eventi di natura accidentale o intenzionale, eventualmente riguardanti anche il proprio personale o per tramite di esso (es. in caso di furto/smarrimento di credenziali/dispositivi) che potrebbero compromettere la sicurezza dei sistemi o dei dati della Committente nonché portare a violazione di obblighi normativi.
- 1.11.12 notifica senza indebito ritardo alla Committente incidenti/anomalie rilevati avendo riguardo a riportare almeno: tipologia e descrizione dell'incidente, componenti (es. reti, sistemi e risorse) coinvolti; l'impatto (anche potenziale) in termini di riservatezza, integrità o disponibilità e ogni altra informazione ritenuta rilevante.
- 1.11.13 si rende disponibile, per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, a svolgere tutte le azioni necessarie per evitare la compromissione dei sistemi o dei dati della Committente nonché la violazione di obblighi normativi; inoltre mette in atto tutti gli interventi opportuni per evitare il ripetersi dell'accaduto in futuro.

**Ove applicabili, nel caso in cui per l'esecuzione delle prestazioni oggetto del Contratto sono previste attività di supporto consulenziale o supporto per la progettazione di soluzioni in ambito tecnologico informatico IT, OT e di sicurezza il Fornitore, ove applicabile per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, assicura il rispetto delle condizioni di sicurezza specifiche di seguito definite, impegnandosi ad integrarle ulteriormente sulla base di una valutazione complessiva di rischio effettuata dalla Committente . In particolare:**



- 1.11.14 adotta un modello di governance per la selezione e designazione del personale che eventualmente opera su risorse messe a disposizione da parte della Committente redigendo e aggiornando un elenco contenente gli estremi identificativi da poter mettere a disposizione della stessa su richiesta. In particolare, effettua una valutazione sull'esperienza, sulla capacità e sull'affidabilità delle figure professionali e comunica senza indebito ritardo alla Committente eventuali situazioni che potrebbero comportare la necessità di revocare autorizzazioni di accesso del proprio personale agli asset e risorse oggetto del presente contratto.
- 1.11.15 garantisce di aver posto in essere e di continuare a porre in essere tutte le azioni necessarie per un corretto provisioning/deprovisioning di tutto il personale del Fornitore che eventualmente opera su risorse messe a disposizione da parte della Committente nel rispetto delle procedure di abilitazione, modifica e revoca degli accessi logici agli asset e alle risorse della stessa.
- 1.11.16 in relazione all'accesso logico, accetta il tracciamento e monitoraggio dei log parte della Committente finalizzato a garantire adeguati controlli di sicurezza sulle operazioni svolte dal personale del Fornitore che eventualmente opera su risorse messe a disposizione da parte della Committente
- 1.11.17 per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, adotta misure di sicurezza anche organizzative per far sì che:
- le credenziali ricevute dal proprio personale che eventualmente opera su risorse messe a disposizione da parte della Committente vengano correttamente custodite esclusivamente dalla figura professionale identificata al fine di evitare l'accesso a tali informazioni da parte di soggetti non formalmente autorizzati;
  - gli accessi del proprio personale che eventualmente opera su risorse messe a disposizione da parte della Committente avvengano unicamente attraverso i canali e gli strumenti e messi a disposizione dalla stessa (es. Virtual Private Network per accessi remoti, accesso con doppio fattore ove ritenuto necessario, ecc.) al fine di garantire che anche eventuali dispositivi utilizzati dal Fornitore siano preventivamente identificati e accedano alle sole risorse per cui sono autorizzati;
  - lo svolgimento delle attività eventualmente svolte dal proprio personale in qualità di utenti con privilegi di amministrazione sui sistemi della Committente avvenga esclusivamente nel rispetto della normativa di riferimento e sulla base delle procedure definite dalla Committente, tra cui accesso tramite piattaforma di mediazione e tracciamento delle attività privilegiate, nonché meccanismi di autenticazione a più fattori e in generale nel rispetto delle indicazioni definite in appositi documenti operativi predisposti dalla Committente.
- 1.11.18 garantisce che tutti i dispositivi utilizzati dal proprio personale per le prestazioni oggetto del contratto (es. pc fissi e portatili) siano sempre aggiornati, mantenuti e ben configurati, a perfetta regola d'arte, condizione necessaria per poter



accedere agli asset e risorse della stessa. In particolare, i dispositivi prevedono quanto meno:

- autenticazione basata su codice di identificazione unico e personale ("User ID") e credenziali ("password") segrete con configurazioni specifiche riguardanti lunghezza, complessità, storicità e durata nel rispetto dei principali standard, utilizzata e conservata esclusivamente dal soggetto a cui è affidata la postazione;
- chiusura automatica delle sessioni utente interattive dopo un intervallo di tempo configurato;
- dotazione di un software antivirus/anti-malware sempre aggiornato all'ultima versione disponibile, non disattivabile dall'utente;
- sistemi firewall e antintrusione per il controllo e il rilevamento di connessioni e accessi non autorizzati (es. firewall del pc abilitato);
- meccanismi/software attivi per la cifratura del disco dati;
- aggiornamento, automatico o manuale, del sistema operativo alle ultime versioni.

- 1.11.19 si adopera per intercettare attraverso presidi e processi di controllo e monitoraggio, incidenti/anomalie, intesi come eventi di natura accidentale o intenzionale, eventualmente riguardanti anche il proprio personale o per tramite di esso (es. in caso di furto/smarrimento di credenziali/dispositivi) che potrebbero compromettere la sicurezza dei sistemi o dei dati della Committente nonché portare a violazione di obblighi normativi.
- 1.11.20 notifica senza indebito ritardo alla Committente incidenti/anomalie rilevati avendo riguardo a riportare almeno: tipologia e descrizione dell'incidente, componenti (es. reti, sistemi e risorse) coinvolti; l'impatto (anche potenziale) in termini di riservatezza, integrità o disponibilità e ogni altra informazione ritenuta rilevante.
- 1.11.21 si rende disponibile, per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, a svolgere tutte le azioni necessarie per evitare la compromissione dei sistemi o dei dati della Committente nonché la violazione di obblighi normativi; inoltre mette in atto tutti gli interventi opportuni per evitare il ripetersi dell'accaduto in futuro.

**Ove applicabili, nel caso in cui l'esecuzione delle prestazioni oggetto del Contratto riguarda la fornitura di soluzioni software "As a Service" (es. servizi in cloud SaaS, PaaS e soluzioni software di elaborazione dati As a Service), erogate direttamente dal Fornitore o tramite il ricorso ad ulteriori terze parti, si impegna a rendere disponibili le certificazioni in ambito cyber (ad esempio ISO 27001, PCI -DSS, SOC-1 etc.) anche per il Cloud Datacenter (ISO27001, CSA CCM, SSAE-16/ISAE3402).** Il Fornitore, ove applicabile per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, assicura il rispetto delle condizioni di sicurezza specifiche di seguito definite, impegnandosi ad integrarle ulteriormente sulla base di una valutazione complessiva di rischio effettuata dalla Committente. In particolare:

- 1.11.22 adotta un modello di governance per la selezione e designazione del proprio personale che opera sulle componenti tecnologiche della soluzione / servizio oggetto del contratto, effettuando una valutazione sull'esperienza, sulla capacità e sull'affidabilità delle figure professionali, redigendo e aggiornando un elenco contenente gli estremi identificativi, che nel caso di personale con privilegi di amministrazione viene messo a disposizione della Committente su richiesta. Il Fornitore rende edotta la Committente circa la presenza di altri service provider, coinvolti nell'erogazione dei servizi cloud contrattualizzati e garantisce l'identificazione di tutti i provider e di tutti i servizi nella catena di outsourcing fornendo chiarimenti se richiesti del fatto i dati rimarranno sotto il suo controllo, oppure se questi svolga un ruolo di intermediario, ovvero offrirà un servizio basato sulle tecnologie messe a disposizione da altro provider.
- 1.11.23 applica specifici processi per la gestione delle identità digitali in grado di garantire adeguati meccanismi di controllo accessi e autenticazione per un corretto e tracciabile provisioning/de-provisioning di tutto il personale autorizzato ad accedere alle componenti tecnologiche sistemistiche e applicative della soluzione / servizio oggetto del contratto nel rispetto di adeguate procedure di abilitazione, modifica e revoca dei permessi e dei privilegi. A tal proposito con riferimento agli accessi eseguiti dal personale della Committente si rende disponibile a prevedere l'integrazione della soluzione / servizio con i sistemi di Identity and Access Governance della Committente stessa.
- 1.11.24 con riferimento a tutto il personale autorizzato ad accedere alle diverse componenti tecnologiche sistemistiche e applicative della soluzione / servizio oggetto del contratto assicura:
- identificazione univoca e gestione delle credenziali con configurazioni specifiche riguardanti lunghezza, complessità, storicità e durata che rispettino le policy definite dalla Committente e in generale i principali standard di settore;
  - accesso eseguito tramite meccanismi di autenticazione a più fattori e limitazione alle sole risorse necessarie oggetto del contratto, sulla base del ruolo assegnato, e nel rispetto dei principii del "Minimo Privilegio", del "Segregazione dei Ruoli" e del "Need to Know";
  - limitazione ad un numero specifico di tentativi di accesso non autorizzato e configurazioni di sicurezza delle sessioni, tra cui ad esempio chiusura automatica dopo uno specifico intervallo di tempo.
- 1.11.25 adotta processi specifici per la verifica periodica del proprio personale che accede ai sistemi e alle componenti informatiche della soluzione / servizio assicurando un adeguata attribuzione delle utenze e dei relativi privilegi e ruoli assegnati. A garanzia delle procedure messe in atto, su richiesta della Committente, previo congruo preavviso, il Fornitore metterà a disposizione reportistica specifica relativamente alle procedure e attività di identity and access management svolte sulla soluzione / servizio oggetto del contratto.
- 1.11.26 assicura che lo svolgimento delle attività in qualità di utenti con privilegi di amministrazione sulle componenti tecnologiche sistemistiche della soluzione / servizio avvenga esclusivamente nel rispetto della normativa di riferimento

nonché di policy specifiche in cui sia garantito, in linea con le baseline della Committente: l'identificazione e il censimento aggiornato di tali utenti, la presenza di meccanismi di autenticazione a più fattori, la presenza di soluzioni intermediazione per il tracciamento e l'archiviazione sicura delle attività svolte, attività di controllo e verifica dell'operativo di tali utenti da poter mettere a disposizione della Committente su richiesta.

- 1.11.27 garantisce che tutti i dispositivi utilizzati dal proprio personale che accede alle componenti tecnologiche della soluzione / servizio oggetto del contratto siano sempre aggiornati, mantenuti e ben configurati, a perfetta regola d'arte nel rispetto dei principi definiti dagli standard di settore, tra cui: autenticazione basata su codice di identificazione unico e personale ("User ID") e credenziali ("password") segrete con configurazioni specifiche riguardanti lunghezza, complessità, storicità e durata nel rispetto dei principali standard, chiusura automatica delle sessioni utente interattive dopo un intervallo di tempo configurato, dotazione di un software antivirus/anti-malware sempre aggiornato all'ultima versione disponibile, non disattivabile dall'utente, presenza di sistemi firewall e anti-intrusione per il controllo e il rilevamento di connessioni e accessi non autorizzati (es. firewall del pc abilitato), aggiornamento del sistema operativo alle ultime versioni.
- 1.11.28 esegue tutte le azioni necessarie per garantire che tutte le componenti tecnologiche della soluzione / servizio siano appositamente censite e adottino requisiti di sicurezza valutati durante l'intero ciclo di vita degli stessi e applicati sin dalla fase di progettazione e sviluppo, fino alla produzione e immissione sul mercato. A tal proposito assicura l'attuazione di processi di security & privacy by design e il rispetto dei principi del Secure code / software development lifecycle, richiamati dalle principali best practices di settore quale ad esempio l'Owasp, in tutti gli interventi di configurazione, sviluppo, manutenzione e/o aggiornamento che riguardano le componenti tecnologiche della soluzione / servizio oggetto del contratto prevedendo una fase di verifica preliminare in un ambiente di test prima dell'effettivo impiego dei medesimi nell'ambiente operativo.
- 1.11.29 esegue con regolarità Vulnerability Assessment e/o Penetration Test al fine di testare la resilienza della soluzione / servizio oggetto del contratto e individuare potenziali vulnerabilità che potrebbero portare a violazioni o incidenti di sicurezza, e formalizza in appositi report l'esito dell'attività di test ed eventuali azioni di remediation intraprese. Il Fornitore mette a disposizione della Committente la documentazione necessaria per attestare l'effettivo svolgimento dell'attività, l'ambito di riferimento ed eventuali piani di rimedio. Ove possibile, si adopera per permettere alla Committente stessa di eseguire test di sicurezza al fine di rilevare vulnerabilità e/o falle di sicurezza sulla soluzione / servizio oggetto del contratto.
- 1.11.30 risolve vulnerabilità e/o falle di sicurezza sulle componenti tecnologiche della soluzione / servizio oggetto del contratto attraverso l'installazione di specifiche patch o con interventi di remediation eseguiti senza indebito ritardo. Ove prevista la messa a disposizione di componenti tecnologiche (es. server, periferiche, apparati di comunicazione, software, ecc.) il Fornitore esegue controlli atti a

identificare e documentare vulnerabilità di tali componenti prima della messa in esercizio, assicurando che le stesse siano aggiornate in conformità con i piani di manutenzione e supporto definiti dai produttori, garantendo così una tempestiva capacità di risposta all'evoluzione delle minacce e delle vulnerabilità informatiche.

- 1.11.31 garantisce di aver posto in essere e di continuare a porre in essere tutte le misure di sicurezza per la protezione della riservatezza, integrità e disponibilità dei dati e delle componenti tecnologiche della soluzione / servizio oggetto del contratto. A tal proposito adotta tutti i meccanismi necessari per: proteggere i flussi di scambio dati attraverso protocolli web sicuri quali ad esempio l'HTTPS; configurare i flussi di accesso e interazione alla soluzione / servizio secondo best practice di sicurezza e ridurre al massimo il livello di esposizione (es. restringere le porte e gli indirizzi IP raggiungibili, separare le connessioni API per fini di amministrazione dalle connessioni funzionali, ecc.); controllare le connessioni e gli accessi alla soluzione / servizio rilevando e bloccando connessioni non autorizzate attraverso soluzioni specifiche tra cui ad esempio web application firewall, anti distributed denial of service; garantire l'adozione di certificati in ambiente cloud validi (es. SSL validi non scaduti, non revocati, etc.); abilitare la funzionalità di data encryption sulle basi dati, prevedendo la possibilità di concedere alla Committente la gestione delle chiavi crittografiche (es. generazione, archiviazione, accesso, cancellazione) per la protezione dei dati appartenenti a quest'ultima; effettuare, amministrare e testare periodicamente soluzioni e processi di backup per il ripristino dei dati della Committente da proteggere con misure specifiche di cifratura; assicurare procedure di ripristino della soluzione / servizio coinvolti garantendone la continuità in caso di eventuali incidenti e/o eventi avversi secondo i livelli di servizio previsti contrattualmente. Il fornitore si impegna a comunicare alla Committente, con un preavviso di almeno 30 giorni, la necessità di spostamento delle risorse e dei dati (compresi i backup) da un sito/data center (suo o di terze parti) ad un altro a implementare nel nuovo centro le stesse misure di sicurezza del sito primario. Resta comunque inteso che lo spostamento delle risorse e dei dati da un sito/data center (suo o di terze parti) ad un altro deve essere preventivamente autorizzato dalla Committente;
- 1.11.32 garantisce di aver posto in essere e di continuare a porre in essere tutti i meccanismi di monitoraggio e controllo degli eventi di sicurezza per intercettare incidenti/anomalie, intesi come eventi di natura accidentale o intenzionale che potrebbero compromettere la riservatezza, l'integrità e la disponibilità dei dati, dei sistemi e delle componenti tecnologiche della soluzione / servizio nonché portare a violazione di obblighi normativi. A tal proposito, se richiesto, prevede la possibilità di attivare l'integrazione della soluzione / servizio oggetto del contratto con le piattaforme di sicurezza della Committente, tra cui Security Incident Event Management (SIEM) e Cloud Access Security Broker (CASB). Per le componenti tecnologiche per cui l'integrazione non risulti possibile, il Fornitore garantisce l'attivazione di processi e meccanismi di monitoraggio, controllo e alerting sui log/eventi di sicurezza attraverso proprie piattaforme di collezionamento e

correlazione, segnalando senza indebito ritardo al Cyber Security Operation Center della Committente, attraverso la casella [iris@a2a.it](mailto:iris@a2a.it), incidenti/anomalie rilevanti per la sicurezza avendo riguardo a riportare almeno: tipologia e descrizione dell'incidente, componenti (es, reti, sistemi e risorse) coinvolti; l'impatto (anche potenziale) in termini di riservatezza, integrità o disponibilità e ogni altra informazione ritenuta rilevante; intervenire, in collaborazione con la Committente, con azioni mirate e piani di risposta e di recupero, volti a eliminare gli effetti degli avvenimenti o, in subordine, a mitigarli. A tal riguardo, il Fornitore garantisce che il suo personale e tutti i suoi collaboratori - inclusi Terzi comunque denominati coinvolti nell'erogazione dei servizi – siano a conoscenza del proprio ruolo e delle operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente ed esegue specifiche esercitazioni con cadenza periodica.

**Ove applicabili, nel caso in cui l'esecuzione delle prestazioni oggetto del Contratto riguarda la fornitura di soluzioni infrastrutturali "As a Service" (es. servizi in cloud IaaS), erogate direttamente dal Fornitore o tramite il ricorso ad ulteriori terze parti, si impegna a rendere disponibili le certificazioni in ambito cyber (ad esempio ISO 27001, PCI -DSS, SOC-1 etc.) anche per il Cloud Datacenter (ISO27001, CSA CCM, SSAE-16/ISAE3402).** Il Fornitore, ove applicabile per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, assicura il rispetto delle condizioni di sicurezza specifiche di seguito definite, impegnandosi ad integrarle ulteriormente sulla base di una valutazione complessiva di rischio effettuata dalla Committente. In particolare:

- 1.11.33 adotta un modello di governance per la selezione e designazione del proprio personale che opera sulle componenti tecnologiche della soluzione / servizio oggetto del contratto, effettuando una valutazione sull'esperienza, sulla capacità e sull'affidabilità delle figure professionali, redigendo e aggiornando un elenco contenente gli estremi identificativi, che nel caso di personale con privilegi di amministrazione viene messo a disposizione della Committente su richiesta. Il Fornitore rende edotta la Committente circa la presenza di altri service provider, coinvolti nell'erogazione dei servizi cloud contrattualizzati e garantisce l'identificazione di tutti i provider e di tutti i servizi nella catena di outsourcing fornendo chiarimenti se richiesti sul fatto che i dati rimarranno sotto il suo controllo, oppure se questi svolga un ruolo di intermediario, ovvero offrirà un servizio basato sulle tecnologie messe a disposizione da altro provider.
- 1.11.34 applica specifici processi per la gestione delle identità digitali in grado di garantire adeguati meccanismi di controllo accessi e autenticazione per un corretto e tracciabile provisioning/de-provisioning di tutto il personale autorizzato ad accedere alle componenti tecnologiche della soluzione / servizio oggetto del contratto nel rispetto di adeguate procedure di abilitazione, modifica e revoca dei permessi e dei privilegi. A tal proposito, ove possibile, si rende disponibile a prevedere l'integrazione della soluzione / servizio con i sistemi di Identity and Access Governance della Committente stessa.



- 1.11.35 con riferimento a tutto il personale autorizzato ad accedere alle diverse componenti tecnologiche della soluzione / servizio oggetto del contratto assicura:
- identificazione univoca e gestione delle credenziali con configurazioni specifiche riguardanti lunghezza, complessità, storicità e durata che rispettino le policy definite dalla Committente e in generale i principali standard di settore;
  - accesso eseguito tramite meccanismi di autenticazione a più fattori e limitazione alle sole risorse necessarie oggetto del contratto, sulla base del ruolo assegnato, e nel rispetto dei principi del “Minimo Privilegio”, del “Segregazione dei Ruoli” e del “Need to Know”;
  - limitazione ad un numero specifico di tentativi di accesso non autorizzato e configurazioni di sicurezza delle sessioni, tra cui ad esempio chiusura automatica dopo uno specifico intervallo di tempo.
- 1.11.36 adotta processi specifici per la verifica periodica del proprio personale che accede ai sistemi e alle componenti informatiche della soluzione / servizio assicurando un adeguata attribuzione delle utenze e dei relativi privilegi e ruoli assegnati.
- 1.11.37 assicura che lo svolgimento delle attività in qualità di utenti con privilegi di amministrazione sulle componenti tecnologiche della soluzione / servizio avvenga esclusivamente nel rispetto della normativa di riferimento nonché di policy specifiche in cui sia garantito, in linea con le baseline della Committente: l'identificazione e il censimento aggiornato di tali utenti, la presenza di meccanismi di autenticazione a più fattori, la presenza di soluzioni intermediazione per il tracciamento e l'archiviazione sicura delle attività svolte, attività di controllo e verifica dell'operativo di tali utenti da poter mettere a disposizione della Committente su richiesta.
- 1.11.38 garantisce che tutti i dispositivi utilizzati dal proprio personale che accede alle componenti tecnologiche della soluzione / servizio oggetto del contratto siano sempre aggiornati, mantenuti e ben configurati, a perfetta regola d'arte nel rispetto dei principi definiti dagli standard di settore, tra cui: autenticazione basata su codice di identificazione unico e personale ("User ID") e credenziali ("password") segrete con configurazioni specifiche riguardanti lunghezza, complessità, storicità e durata nel rispetto dei principali standard, chiusura automatica delle sessioni utente interattive dopo un intervallo di tempo configurato, dotazione di un software antivirus/anti-malware sempre aggiornato all'ultima versione disponibile, non disattivabile dall'utente, presenza di sistemi firewall e anti-intrusione per il controllo e il rilevamento di connessioni e accessi non autorizzati (es. firewall del pc abilitato), aggiornamento del sistema operativo alle ultime versioni.
- 1.11.39 esegue tutte le azioni necessarie per garantire che tutte le componenti tecnologiche della soluzione / servizio siano appositamente censite e adottino requisiti di sicurezza valutati durante l'intero ciclo di vita degli stessi e applicati sin dalla fase di progettazione e sviluppo, fino alla produzione e immissione sul mercato. A tal proposito assicura l'attuazione di processi di security & privacy by

design e il rispetto dei principi del Secure code / software development lifecycle, richiamati dalle principali best practices di settore quale ad esempio l'Owasp, in tutti gli interventi di configurazione, sviluppo, manutenzione e/o aggiornamento che riguardano le componenti tecnologiche della soluzione / servizio oggetto del contratto prevedendo una fase di verifica preliminare in un ambiente di test prima dell'effettivo impiego dei medesimi nell'ambiente operativo.

- 1.11.40 valuta il rischio di sicurezza derivante dallo sfruttamento di caratteristiche dei sistemi e delle componenti tecnologiche oggetto del contratto ed effettua opportuni test di verifica volti ad individuare vulnerabilità/problematiche di sicurezza provvedendo al rimedio delle stesse prima della messa in esercizio e/o assicurando che le stesse siano aggiornate in conformità con i piani di manutenzione e supporto definiti dai produttori, garantendo così una tempestiva capacità di risposta all'evoluzione delle minacce e delle vulnerabilità informatiche. e/o nei tempi concordati con la Committente.
- 1.11.41 esegue tutte le azioni necessarie per garantire che sistemi e componenti informatiche oggetto del presente contratto siano conformi a tutti i requisiti necessari a prevenire gli incidenti di sicurezza valutati durante l'intero ciclo di vita degli stessi e applicati sin dalla fase di progettazione e sviluppo, fino alla produzione e immissione sul mercato. A tal proposito assicura l'attuazione dei principi di security by design e di Secure Software Development Lifecycle in tutti gli eventuali interventi di sviluppo, manutenzione e/o aggiornamento che riguardano i sistemi e le componenti informatiche oggetto del contratto garantendo una fase di verifica preliminare in un ambiente di test prima dell'effettivo impiego dei medesimi nell'ambiente operativo nonché l'adozione di best practice di settore (es. OWASP)
- 1.11.42 segnala tempestivamente e in qualsiasi momento alla Committente ogni situazione, vulnerabilità e/o problematica di sicurezza di cui è a conoscenza che potrebbe riguardare le componenti tecnologiche oggetto del contratto, fornendo indicazione ed intervenendo con remediation e azioni di patching/hardening al fine di non compromettere la capacità della Committente di garantire un adeguato livello di sicurezza nello svolgimento dei propri servizi.
- 1.11.43 garantisce di aver posto in essere e di continuare a porre in essere tutte le misure di sicurezza per la protezione delle componenti tecnologiche oggetto del presente contratto. A tal proposito adotta tutti i meccanismi necessari per: controllare le connessioni e gli accessi bloccando connessioni non autorizzate attraverso soluzioni specifiche di anti distributed denial of service; prevedere processi e procedure di high availability e l'adozione di strumenti ridondati per garantire attraverso la sincronizzazione in tempo reale la resistenza dei sistemi e delle componenti informatiche oggetto del contratto a errori e/o malfunzionamenti. Il fornitore si impegna a comunicare alla Committente, con un preavviso di almeno 30 giorni, la necessità di spostamento delle risorse e dei dati (compresi i backup) da un sito/data center (suo o di terze parti) ad un altro a implementare nel nuovo centro le stesse misure di sicurezza del sito primario. Resta comunque inteso che lo spostamento delle risorse e dei



dati da un sito/data center (suo o di terze parti) ad un altro deve essere preventivamente autorizzato dalla Committente;

- 1.11.44 garantisce di aver posto in essere e di continuare a porre in essere tutti i meccanismi di monitoraggio e controllo degli eventi di sicurezza per intercettare incidenti/anomalie, intesi come eventi di natura accidentale o intenzionale che potrebbero compromettere la riservatezza, l'integrità e la disponibilità dei dati, dei sistemi e delle componenti tecnologiche della soluzione / servizio nonché portare a violazione di obblighi normativi. A tal proposito, se richiesto, prevede la possibilità di attivare l'integrazione della soluzione / servizio oggetto del contratto con le piattaforme di sicurezza della Committente, tra cui Security Incident Event Management (SIEM) e Cloud Access Security Broker (CASB). Per le componenti tecnologiche per cui l'integrazione non risulti possibile, il Fornitore garantisce l'attivazione di processi e meccanismi di monitoraggio, controllo e alerting sui log/eventi di sicurezza attraverso proprie piattaforme di collezionamento e correlazione, segnalando senza indebito ritardo al Cyber Security Operation Center della Committente, attraverso la casella [iris@a2a.it](mailto:iris@a2a.it), incidenti/anomalie rilevanti per la sicurezza avendo riguardo a riportare almeno: tipologia e descrizione dell'incidente, componenti (es, reti, sistemi e risorse) coinvolti; l'impatto (anche potenziale) in termini di riservatezza, integrità o disponibilità e ogni altra informazione ritenuta rilevante; intervenire, in collaborazione con la Committente, con azioni mirate e piani di risposta e di recupero, volti a eliminare gli effetti degli avvenimenti o, in subordine, a mitigarli. A tal riguardo, il Fornitore garantisce che il suo personale e tutti i suoi collaboratori - inclusi Terzi comunque denominati coinvolti nell'erogazione dei servizi – siano a conoscenza del proprio ruolo e delle operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente ed esegue specifiche esercitazioni con cadenza periodica.

**Ove applicabili, nel caso in cui l'esecuzione delle prestazioni oggetto del Contratto riguarda la fornitura di prodotti hardware e relativi sistemi di elaborazione (es. apparati di rete, server, soluzioni di elaborazione, ecc.),** il Fornitore, ove applicabile per quanto di propria specifica competenza ed in relazione al servizio effettivamente svolto, assicura il rispetto delle condizioni di sicurezza specifiche di seguito definite, impegnandosi ad integrarle ulteriormente sulla base di una valutazione complessiva di rischio effettuata dalla Committente . In particolare:

- 1.11.45 esegue tutte le azioni necessarie per garantire che il prodotto oggetto del presente contratto siano conformi a tutti i requisiti necessari a prevenire gli incidenti di sicurezza valutati durante l'intero ciclo di vita degli stessi e applicati sin dalla fase di progettazione e sviluppo, fino alla produzione e immissione sul mercato.
- 1.11.46 valuta il rischio di sicurezza derivante dallo sfruttamento di caratteristiche del prodotto oggetto del presente contratto ed effettua opportuni test di verifica volti ad individuare vulnerabilità/problematiche di sicurezza provvedendo al rimedio delle stesse prima della messa in esercizio e/o della fornitura alla Committente.

- 1.11.47 esegue adeguati controlli periodici atti a identificare e documentare vulnerabilità sul prodotto oggetto del presente contratto assicurando che tutte le componenti siano aggiornati prima della messa in esercizio e nel corso dell'esercizio delle stesse (ove previsto) in conformità con i piani di manutenzione e supporto definiti da eventuali ulteriori produttori, garantendo così una tempestiva capacità di risposta all'evoluzione delle minacce e delle vulnerabilità informatiche.
- 1.11.48 segnala tempestivamente e in qualsiasi momento alla Committente ogni situazione, vulnerabilità e/o problematica di sicurezza di cui è a conoscenza che potrebbe riguardare i prodotti oggetto del presente contratto, fornendo indicazione di remediation in termini di patching/hardening delle stesse al fine di non compromettere la capacità della Committente di garantire un adeguato livello di sicurezza nello svolgimento dei propri servizi.