Allegato ----- al contratto n° -----

SICUREZZA DELLE INFORMAZIONI / CYBERSECURITY

1 Campo d'applicazione, obiettivi e contenuti

1.1 Il presente allegato si applica a tutte le prestazioni dell'Azienda, da essa eseguite o fornite nell'ambito del presente contratto. L'allegato descrive i requisiti minimi e gli obblighi dell'Azienda volti alla riduzione dei cyber-rischi (di seguito sono intesi con il medesimo significato anche i rischi per la sicurezza delle informazioni) e integra i requisiti della relativa legislazione, nonché ulteriori requisiti specifici in funzione del cliente e del luogo d'impiego.

1.2 Nel presente allegato, i termini «sicurezza», «sicuro» o «rilevante per la sicurezza» si riferiscono alla protezione e alla resilienza rispetto alla sicurezza delle informazioni o ai cyber-rischi. L'area della sicurezza funzionale (safety) non fa parte di questo allegato.

2 Gestione della sicurezza

2.1 L'Azienda mantiene un sistema di gestione della sicurezza aziendale per la riduzione dei cyber-rischi adatto per tipo e portata alla prestazione da fornire e conforme allo stato della tecnica riconosciuto (ad es. secondo ISO/IEC 27001 o IEC 62443- 2-1).

2.2 L'Azienda garantisce che i propri collaboratori e i collaboratori dei subappaltatori coinvolti nello sviluppo e nella produzione dei prodotti e dei componenti o impiegati per fornire i servizi siano sensibilizzati e formati in merito ai cyber-rischi, conoscano le relative prescrizioni e la loro integrità sia stata opportunamente e sia regolarmente controllata. Essa garantisce inoltre che questi collaboratori utilizzino i loro diritti di accesso ai sistemi e ai dati delle FFS esclusivamente per adempiere ai loro obblighi contrattuali.

2.3 Nell'ambito dello sviluppo di software e prodotti, l'Azienda implementa processi volti a ridurre i cyber-rischi. Tali processi si basano sui principi di «security by design» e «privacy by design», qualora siano trattati dati personali. L'Azienda segue metodi e standard riconosciuti, come IEC 62443- 4-1 o NIST SP 800-160.

2.4 Per la comunicazione di vulnerabilità, l'Azienda dispone di direttive e processi conformi a metodi e standard riconosciuti, come ISO/IEC 29147. I processi e le direttive comprendono, in particolare, le definizioni delle modalità secondo cui possono essere effettuate le segnalazioni di vulnerabilità, sono valutate le stesse e le informazioni sulle vulnerabilità sono comunicate alla FFS SA.

2.5 L'Azienda dispone dei processi necessari per trattare le vulnerabilità e segue metodi e standard riconosciuti (ad es. ISO/IEC 30111).

3 Persona di contatto per la cybersecurity

3.1 Le parti indicano una persona di contatto responsabile del coordinamento delle intese, del controllo del rispetto dei requisiti del presente allegato e di ulteriori accordi.

3.2 Le parti garantiscono che la sostituzione delle persone di contatto nel corso della durata del progetto e durante il periodo di manutenzione del prodotto siano comunicati alla rispettiva controparte in modo tempestivo.

3.3 Per eventuali domande riguardanti la cybersecurity, l'Azienda comunica un contatto generale raggiungibile anche dopo la scadenza del contratto.

4 Incidenti di sicurezza

4.1 L'Azienda informa immediatamente la FFS SA in caso di incidenti di sicurezza rilevanti (incidents).

4.2 L'Azienda fornisce assistenza alla FFS SA in caso di incidenti concernenti la cybersecurity legati ai suoi prodotti e servizi.

4.3 L'Azienda si impegna a fornire un logging adeguato dei sistemi e dei prodotti al fine di consentirne l'integrazione in un sistema di monitoraggio centrale. Se i dati di log sono gestiti dall'Azienda, essa fornisce alla FFS SA i relativi rapporti di sicurezza e garantisce che i dati di log siano conservati per un periodo di tempo sufficiente.

4.4 In caso di incidenti di sicurezza rilevanti per la FFS SA, vengono messi a disposizione tutti i dati e tutti i documenti necessari per una rapida risoluzione dell'incidente.

5 Gestione delle vulnerabilità e delle patch

5.1 L'Azienda informa proattivamente la FFS SA in merito alle vulnerabilità rilevanti.

5.2 Il prodotto o il servizio prevede la possibilità di correggere eventuali errori del software (compresi firmware e sistema operativo) che comportano un cyber-rischio. Il software (compreso il firmware e il sistema operativo) può essere adeguatamente aggiornato a tal fine.

5.3 L'Azienda dispone di un processo prestabilito per fornire aggiornamenti dei software. Il processo include le misure necessarie per garantire l'autenticità e l'integrità degli aggiornamenti software forniti.

5.4 L'Azienda garantisce che gli aggiornamenti dei software che concernono vulnerabilità in materia di cybersecurity sono forniti o applicati in modo tempestivo.

6 Consegna, documentazione ed esercizio

6.1 Quando l'Azienda consegna dei prodotti, deve fornire alla FFS SA tutta la documentazione necessaria per l'integrazione e l'esercizio sicuri del prodotto. Ciò include, ad esempio, documenti relativi all'architettura, informazioni sugli algoritmi crittografici utilizzati, materiale chiave, account utente e password. I documenti devono essere trasmessi mediante canali o depositi sicuri.

6.2 Al momento della consegna di software e relativi aggiornamenti, l'Azienda fornisce i mezzi necessari, come i checksum, per verificare l'autenticità e l'integrità della consegna.

6.3 Le condizioni dell'ambiente, le impostazioni e le fasi di messa in esercizio necessarie per l'esercizio sicuro del prodotto sono chiaramente indicate nella documentazione. La documentazione deve essere sempre aggiornata durante tutto il ciclo di vita del prodotto.

6.4 Gli accessi per la manutenzione ai sistemi della FFS SA devono essere sempre dichiarati e concordati. Ove possibile ed economicamente sostenibile, si devono utilizzare gli accessi di manutenzione standard della FFS SA.

7 Collaudo

7.1 Salvo diversamente disciplinato nel contratto o nelle CG, si applicano le seguenti regole specifiche per il collaudo.

7.2 Per il collaudo, la FFS SA può richiedere verifiche di sicurezza specifiche, come un test di penetrazione, da parte di esperti interni o esterni.

7.3 Se dalla verifica emergono solo vulnerabilità non critiche, il collaudo avrà comunque luogo alla conclusione della verifica. L'Azienda correggerà immediatamente le vulnerabilità individuate e comunicherà alla FFS SA la loro eliminazione.

7.4 Qualora durante le verifiche di sicurezza emergano vulnerabilità critiche, il collaudo sarà rimandato. L'Azienda eliminerà immediatamente le vulnerabilità constatate e inviterà tempestivamente la FFS SA a effettuare una nuova verifica.

7.5 L'inizio dell'uso produttivo dell'opera non costituisce collaudo, salvo in caso di apposita conferma scritta della FFS SA.

7.6 Nonostante il rinvio del collaudo, l'oggetto del contratto può essere lasciato in uso alla FFS SA di comune accordo; in tal caso tutti i diritti e gli obblighi delle parti per quanto riguarda il collaudo e le sue conseguenze giuridiche rimangono in essere.

8 Garanzia

8.1 Le vulnerabilità dei prodotti o dei servizi forniti dall'Azienda, constatate al momento del collaudo o in un momento successivo, sono considerate difetti ai sensi del contratto e si applicano i corrispondenti obblighi di garanzia.

9 Diritto di controllo e di audit da parte delle FFS

9.1 Salvo diversamente disciplinato nel contratto o nelle CG, si applicano le seguenti regole specifiche in merito al diritto di controllo e di audit.

9.2 La FFS SA ha il diritto di esigere che il rispetto degli obblighi dell'Azienda di cui alla cifra «Gestione della sicurezza» e di ulteriori obblighi essenziali siano verificati da un organismo indipendente. La verifica può essere effettuata dalla stessa FFS SA o da una società di revisione indipendente nell'ambito di un audit. Ciascuna parte si assume in tal caso le proprie spese sostenute o commissionate. Senza una buona ragione, la FFS SA non può esigere una simile verifica più di una volta per anno civile.

9.3 Se l'audit non viene effettuato dalla stessa FFS SA, il rapporto di revisione si limita a informare la FFS SA sull'esatta portata della verifica e sul rispetto o meno degli obblighi contrattuali da parte dell'Azienda. In caso di violazione, la FFS SA ha un diritto completo di esaminare le informazioni rilevanti per la violazione. In questo caso, le FFS possono riaddebitare all'Azienda la loro parte di costi (incl. evtl. quelli relativi a imprese incaricate) per la verifica.

9.4 L'Azienda accorda alla FFS SA e ai corrispondenti partner contrattuali della FFS SA il diritto di verificare l'integrità e la sicurezza dell'hardware e del software del prodotto (reverse engineering). Ciò non rappresenta una violazione dei diritti di proprietà intellettuale (DPI) dell'Azienda.

10 Subappaltatori

10.1 Salvo diversamente disciplinato nel contratto o nelle CG, si applicano le seguenti regole specifiche in merito ai subappaltatori.

10.2 Qualora l'Azienda faccia ricorso a terzi per l'adempimento delle proprie prestazioni, incl. la fornitura di prodotti, la quota di fornitura di tali terzi dovrà essere integrata completamente nella gestione della sicurezza dell'Azienda e mostrata alle FFS su richiesta. Essa mantiene un sistema appropriato per l'analisi, la selezione e la valutazione regolare dei subappaltatori.

10.3 L'Azienda fornirà la prova di aver vincolato i terzi da lei coinvolti al rispetto degli impegni da essa assunti nell'ambito del presente allegato oppure assicurerà personalmente, mediante proprie risorse, la cybersecurity delle forniture, anche anticipate. La FFS SA può esigere dall'Azienda prove documentate attestanti che la stessa ha verificato l'efficacia della gestione della sicurezza presso i terzi da essa coinvolti.