

# Addendum Sicurezza Informatica Fornitori

*Condizioni Generali*

Ambito Security e Data Protection

09/06/2023 – Rev. 00

## Sommario

Scopo e Campo di applicazione del Documento.....	
1.1 Classificazione del Documento.....	
1.2 Approvazione, Modifica e Manutenzione del Documento.....	
1.3 Riferimenti Normativi.....	
1.4 Definizioni.....	
2 Sicurezza e Confidenzialità.....	
2.1 Aspetti generali.....	
2.2 Sicurezza del Fornitore.....	
2.3 Gestione delle Informazioni.....	
2.4 Utenze per l'erogazione e accesso al Servizio e alle Informazioni.....	
2.5 Auditing Cybersecurity & Compliance.....	
2.6 Incident e Data Breach Management.....	
2.6.1 Incidenti Cyber.....	
2.6.2 Incidenti di sicurezza con Data Breach.....	
3 Regole di Data Protection.....	
3.1 Il Trattamento dei Dati.....	
3.2 Gestione degli Amministratori di Sistema.....	
3.3 Gestione della conservazione e cancellazione dei dati.....	
3.4 Sistemi del Fornitore per il trattamento di dati.....	
3.5 Protezione delle aree di lavoro.....	
3.6 Requisiti minimi per la protezione degli strumenti di lavoro elettronici.....	
3.7 Accesso da remoto ai dati e alle applicazioni.....	
3.7.1 Accesso da paesi extra EU.....	
3.7.2 Smartworking e attività in Reperibilità.....	
4 Supply Chain Security.....	
Requisiti per fornitura, integrazione o lo sviluppo di applicativi software firmware e/o sistemi	
.....	
5 Fornitura della componente Software.....	
5.1 Authentication, Authorization e Accounting (AAA).....	
5.1.1 Authentication.....	
5.1.2 Authorization.....	
5.1.3 Accounting.....	
5.1.4 Requisiti di Authentication, Authorization e Accounting.....	
5.2 Posizionamento, retention, cancellazione, portabilità dei dati.....	
5.2.1 Portabilità.....	
5.3 Tracciamento degli accessi e delle operazioni, log e monitoraggio.....	
5.3.1 Generazione, conservazione e analisi dei log.....	
5.4 Requisiti per le interfacce WEB.....	
5.5 Requisiti specifici App Mobile.....	
5.6 Requisiti per le interfacce Api.....	

5.7 Data transfer.....	
5.8 Cifratura dei dati memorizzati.....	
5.9 Affidabilità e Backup.....	
6 Sicurezza della componente Hardware e delle infrastrutture, Cloud.....	
6.1 Applicativi posizionati nei data center presso il Fornitore.....	
6.2 Applicativi posizionati al di fuori del perimetro fisico di AULSS n. 9 Scaligera/Fornitore.....	
6.3 Norme per l'utilizzo del Cloud.....	
6.4 Sicurezza di infrastrutture basate su virtualizzazione e/o container.....	
6.4.1 Virtualizzazione.....	
6.4.2 Container.....	
7 Sviluppo Sicuro aggiornamenti e life cycle.....	
7.1 Regole per lo sviluppo sicuro del codice.....	
7.2 Aggiornamento del prodotto software e delle piattaforme.....	
7.3 Gestione degli aggiornamenti del Software.....	
7.3.1 Portale o strumenti del Fornitore per gli aggiornamenti.....	
8 Verifiche di sicurezza su applicativi e sistemi.....	
8.1 Documentazione, verifiche e certificazioni di sicurezza del Fornitore.....	
8.2 AULSS n. 9 Scaligera Security Assessment (VA/PT).....	

# Scopo e Campo di applicazione del Documento

Nel documento "Addendum Sicurezza Informatica" per la fornitura di Beni/Servizi da terze parti (di seguito Addendum) sono descritti i principi generali della sicurezza richiesti da *AULSS n. 9 Scaligera* e applicabili a tutti i contratti/ordini dove i Fornitori:

- Effettuano direttamente o indirettamente trattamento di dati di *AULSS n. 9 Scaligera*;
- Forniscono strumenti per il trattamento di dati (ad esempio piattaforme o applicativi software);
- Forniscono dispositivi come a titolo esemplificativo router, CPE, Server che siano connessi alla rete di *AULSS n. 9 Scaligera*

Questo documento è connesso alle Condizioni Generali allegate al contratto tra *AULSS n. 9 Scaligera* e il Fornitore, e vi sono descritte le politiche, gli obiettivi e i requisiti di sicurezza che sono richiesti da *AULSS n. 9 Scaligera* per la protezione delle informazioni e degli asset fisici e logici che il Fornitore è tenuto a adottare e implementare al fine di garantire l'integrità, la disponibilità e la riservatezza dei dati personali e delle informazioni di *AULSS n. 9 Scaligera*, contemplando anche il livello di protezione degli asset.

Il documento è strutturato in:

- Il documento principale (Addendum) che riferisce a requisiti generali normalmente applicabili ad ogni contratto,
- Alcuni allegati (Annex) applicabili se e solo se l'oggetto inerente alla fornitura le preveda.

Ad esempio, nel caso in cui sia prevista la fornitura, l'implementazione o la realizzazione di software applicativi è obbligatoriamente applicabile l'allegato dedicato (vedi par 1.2).

In generale tutti i requisiti sono da intendersi come "ove applicabili", in funzione del tipo di ordine/contratto e, quindi, alcuni paragrafi potrebbero essere "non applicabili - N/A". Nel caso in cui, data la complessità o particolarità del servizio offerto, dovessero essere necessari requisiti aggiuntivi, si precisa che saranno definiti in un addendum di sicurezza informatica, appositamente scritto e allegato all'ordine/contratto.

Questo addendum sarà redatto in fase di avvio ed esecuzione del progetto con la definizione di specifici meccanismi, accorgimenti o requisiti di sicurezza da implementare e/o integrare.

## 1.1 Classificazione del Documento

Il presente documento è classificato "*Pubblico/Confidenziale*," ed in quanto tale può essere condiviso all'esterno/deve essere soggetto al trattamento da parte del solo personale autorizzato (Management *AULSS n. 9 Scaligera*, oppure Dipartimento XXXXX, Responsabile IT, CISO, Procurement, personale incaricato dello svolgimento dell'attività di analisi).

## 1.2 Approvazione, Modifica e Manutenzione del Documento

Il presente documento è verificato periodicamente ed aggiornato qualora dovessero essere necessarie modifiche sulle modalità operative o del processo di riferimento.

Il documento è redatto dalla funzione di Comitato per la Cyber Security / CISO / DPO / e condiviso con Responsabile Security&Data Protection per l'approvazione.

## 1.3 Riferimenti Normativi

Il Fornitore si impegna ad essere conforme a tutte le normative vigenti che disciplinano le attività oggetto del contratto; in particolare il Fornitore si impegna, se applicabile, ad adempiere a tutti gli obblighi imposti D.Lgs 81/2008 (Sicurezza sui luoghi di lavoro) e dal Regolamento UE 2016/679 (GDPR) e al D.Lgs. 101/2018, comprese le successive integrazioni, e a produrre nei confronti di *AULSS n. 9 Scaligera* i documenti richiesti, nei modi e nelle tempistiche prescritte dalla legge.

Si tenga presente che per le tematiche di Security e Privacy:

- Il Regolamento GDPR è vincolante e deve essere considerato come obbligatorio;
- Le misure di sicurezza delle informazioni esplicitate da *AULSS n. 9 Scaligera* devono essere considerate come integrative a quanto previsto dalle normative di legge;
- Le norme internazionali ISO 27001 e 27002 sono considerate la base per i controlli necessari e per la valutazione del rischio;
- Lo OWASP è preso come riferimento per le applicazioni software e web base;
- Le Linee Guida – Sicurezza nel Procurement ICT (aprile 2020)
- D.Lgs 65 18 maggio 2018, Direttiva (UE) 2016/1148, cd. Direttiva NIS

- D.Lgs 105/2019

Per le linee guida e per verifiche sui temi di sicurezza Cyber, il dipartimento di Security/Comitato per la Cybersecurity, CISO prende come riferimento:

- NIST" (National Institute of Standards e Technology cybersec framework")  
<https://www.nist.gov/cyberframework>
- "Centro di Ricerca di Cyber Intelligence and Information Security" (CIS) dell'Università Sapienza di Roma (Framework Nazionale cybersec) (Italian Version)  
<https://www.cybersecurityframework.it>
- Per la tecnologia 5G si fa riferimento alle indicazioni previste da 5GEnsure e ENISA Un elenco del quadro normativo di riferimento è indicato nell'appendice I.

Il Fornitore si impegna altresì a garantire che le normative indicate siano rispettate, se applicabili, anche dai propri sub-fornitori ed a fornire le informazioni necessarie per le verifiche del rispetto delle normative.

I requisiti indicati in questo documento e i suoi allegati, ove possibile, non obbligano la scelta di una soluzione tecnica ma propongono un gamma di misure alternative, lasciando al Fornitore la possibilità di individuare i meccanismi di sicurezza da implementare, in considerazione del tipo di esposizione ai rischi, fisico o Cyber, della criticità a livello di business e della tipologia d'informazioni scambiate. Potranno essere implementate misure alternative a quanto proposto, previa verifica con *AULSS n. 9 Scaligera*, ma dovranno in ogni caso garantire un livello di sicurezza non inferiore alle soluzioni consigliate e con il pieno soddisfacimento dei requisiti.

## 1.4 Definizioni

In questa sezione viene riportata una spiegazione dei vari termini specifici utilizzati all'interno del/della presente processo/procedura, calati/limitati al contesto/campo di quest'ultimo/ultima. Vengono riportati in ordine alfabetico ordine alfabetico per una più rapida ricerca/consultazione.

BUSINESS CONTINUITY
<p><u><i>BCMS (Business Continuity Management System)</i></u> - Insieme delle politiche, delle procedure, delle buone pratiche e delle attività in carico al BC Team per la gestione della BC in <i>AULSS n. 9 Scaligera</i>. Il BCMS definisce, nel caso di eventi disastrosi, le attività finalizzate alla gestione e al ripristino dei processi a supporto del servizio erogato verso <i>AULSS n. 9 Scaligera</i> fino al rientro alla normalità;</p> <p><u><i>BCP (Business Continuity Plan)</i></u> - Insieme di procedure documentate che guidano l'Azienda nel rispondere ad un incidente disastroso e ripristinare i processi critici a seguito di un'interruzione. Il BCP fornisce indicazioni in merito a: perimetro, obiettivi, ruoli e responsabilità, criteri di attivazione, manutenzione, aggiornamento e test in ambito Business Continuity;</p> <p><u><i>BIA (Business Impact Analysis)</i></u> - Metodologia di analisi che, attraverso la raccolta di informazioni chiave di processi critici di <i>AULSS n. 9 Scaligera</i>, consente di determinare l'impatto e le ricadute sul Business di eventi che causano l'interruzione di tali processi.: CFR ISO/TS 22317:2015 Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA);</p> <p><u><i>Crisis Committee</i></u> - Comitato che si riunisce in caso di Crisi, su richiesta del Crisis Manager. La sua funzione principale è quella di valutare ed eventualmente approvare l'apertura dello stato di crisi;</p> <p><u><i>DR (Disaster Recovery)</i></u> - Insieme delle misure tecnologiche e logistico/organizzative finalizzate al ripristino dei sistemi/dati necessari all'erogazione di un processo erogato a <i>AULSS n. 9 Scaligera</i>;</p> <p><u><i>Evento disastroso/crisi</i></u> - Evento straordinario i cui impatti possono essere tali da minacciare la Mission dell'azienda e/o i suoi obiettivi strategici;</p> <p><u><i>Incidente</i></u> - Evento che può verificarsi nella normale operatività riducendo in alcuni casi la qualità del servizio erogato;</p> <p><u><i>Process Owner</i></u> - Soggetto preposto e responsabile della conduzione operativa di processi di competenza;</p> <p><u><i>RA (Risk Assessment)</i></u> - Processo di identificazione dei rischi e delle vulnerabilità relative alle risorse a supporto di ogni processo critico per il Business identificato in sede di BIA;</p> <p><u><i>RTO (Recovery Time Objective)</i></u> - Obiettivo temporale entro il quale un sistema o un processo organizzativo dovrebbe essere ripristinato;</p> <p><u><i>RPO (Recovery Point Objective)</i></u> - Rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (backup);</p> <p><u><i>MAO (Maximum Acceptable Outage)</i></u> - Limite di tempo superato il quale l'interruzione di un processo critico causa</p>

danni irreparabili all'Azienda;

MBCO (Minimum Business Continuity Objective) - Minimo livello di servizio/operatività che deve essere garantito al momento del ripristino di un processo;

Test di Business Continuity (Test BC) – Test di continuità operativa, finalizzato a verificare l'efficacia del piano di continuità e il rispetto dei tempi di ripristino definiti (RTO);

Test di Disaster Recovery (Test DR) – Test di ripristino delle componenti infrastrutturali e applicative del servizio erogato, finalizzato a verificare l'efficacia delle procedure di ripristino e il rispetto dei tempi di ripristino definiti (RTO).

## 2 Sicurezza e Confidenzialità

### 2.1 Aspetti generali

*AULSS n. 9 Scaligera* in ottemperanza al Regolamento GDPR, ha implementato il processo di Security by design and by default, in quanto è desiderata l'adozione di approcci sistematici e sicuri basati su normative nazionali, standard e framework riconosciuti a livello internazionale, a garanzia della protezione adeguata dei dati e degli asset aziendali.

*AULSS n. 9 Scaligera* per tutti i servizi oggetto di fornitura di terze parti effettua una valutazione del rischio Cyber. Tale valutazione permette di rilevare il rischio strutturale e di individuare le contromisure atte a ridurlo tramite l'adozione di specifiche misure di sicurezza. Nella fase di valutazione la *AULSS n. 9 Scaligera* definirà la necessità o meno di un addendum di sicurezza contenente ulteriori requisiti specifici.

Con l'affidamento di un Servizio/Sistema si evidenzia che il Fornitore stesso diventa, a tutti gli effetti, un partner del ciclo operativo di *AULSS n. 9 Scaligera* e della sua catena del valore. Da ciò deriva l'esigenza di adottare uno specifico processo di analisi e gestione dei rischi, con il coinvolgimento attivo del Fornitore, focalizzato anche su tutti sugli aspetti d'integrazione e di business.

Nel corso della validità del contratto potrebbe rendersi necessaria una nuova valutazione del rischio, a seguito di nuove minacce o del mutamento delle condizioni di applicazione del servizio. Da ciò, su richiesta espressa di *AULSS n. 9 Scaligera*, il Fornitore è tenuto a fornire tutte le informazioni necessarie per consentire una nuova valutazione dei rischi associati al trattamento dei dati, di asset e di informazioni di proprietà. La *AULSS n. 9 Scaligera* A seguito della nuova valutazione, *AULSS n. 9 Scaligera* e il Fornitore dovranno cooperare attivamente per trovare una soluzione congiunta per la riduzione del rischio stesso a livelli accettabili.

In caso in cui modifiche di leggi Italiane o Europee impongano l'adozione di nuovi adempimenti, *AULSS n. 9 Scaligera* è obbligata a uniformarsi alle disposizioni di legge. Nel caso in cui l'adempimento riguardi servizi, software o infrastrutture del Fornitore, questi è obbligato a adempiere a tali disposizioni. Se non dovuto già a termini di legge, il Fornitore si rende disponibile a fornire una valutazione di quanto necessario per consentire a *AULSS n. 9 Scaligera* una conformità alla normativa. Le parti dovranno predisporre l'adeguamento alla normativa in modo autonomo comunicando le modifiche strutturali o di processo alla controparte.

Con l'esecuzione dell'ordine/contratto si intendono applicabili e accettate le clausole di riservatezza definite in essere tra le parti.

### 2.2 Sicurezza del Fornitore

Qualora l'oggetto del contratto preveda il trattamento di Dati Personali di cui *AULSS n. 9 Scaligera* è il Titolare, e/o l'adozione di strumenti informatici, il Fornitore deve esibire informazioni dettagliate sulla propria organizzazione ai fini della gestione della sicurezza delle informazioni, attraverso un documento appositamente redatto detto "Scheda Fornitore - SI", documento che descrive la modalità organizzative del Fornitore relativamente alla sicurezza delle informazioni.

La scheda, inclusa negli allegati del presente Addendum comprendere l'assegnazione di ruoli e responsabilità per:

- Identificare rischi e requisiti di sicurezza;
- Decidere come trattare i rischi e soddisfare i requisiti;
- Identificare le misure di sicurezza;
- Pianificare e attuare tali misure e verificarne l'applicazione e l'efficacia.
- La gestione delle comunicazioni di "change management" da parte di *AULSS n. 9 Scaligera*
- Gestione e pronta comunicazione degli incidenti di sicurezza o data breach e la relativa reportistica
- Comunicazione degli amministratori di sistema (AdS) quanto previsti
- Comunicazione periodica delle vulnerabilità identificate sui sistemi oggetto di fornitura e delle conseguenti patch applicate dal Fornitore;
- Comunicazione tempestiva di eventuali variazioni di rischio residuo

Ad ogni aggiornamento organizzativo dovrà seguire puntuale comunicazione, con la messa in evidenza delle variazioni, in modo da permettere le dovute verifiche e l'adeguamento delle misure di sicurezza a fronte dei cambiamenti, siano essi di natura interna, esterna, di mercato o regolamentare.

Ogni aggiornamento dovrà essere inviato a \_\_\_\_\_ e condiviso con \_\_\_\_\_

Qualora il Servizio venga fornito attraverso l'ausilio di strumenti o soggetti giuridici localizzati fuori dal territorio nazionale, tale informazione dovrà essere descritta nel contratto e il Fornitore dovrà fornire con congruo preavviso ogni elemento utile alla valutazione del caso garantendo in ogni caso il pieno rispetto della normativa vigente, Italiana e Europea.

## 2.3 Gestione delle Informazioni

*AULSS n. 9 Scaligera* ha classificato le proprie informazioni ed il loro livello di riservatezza, ed assicura a utenti, clienti ed ogni stakeholder che dati personali, informazioni di business, e documenti e strumenti con i quali questi sono trattati siano adeguatamente protette a ogni livello.

Il Fornitore si impegna a gestire informazioni e documenti di *AULSS n. 9 Scaligera* la diligenza atta a conservare la protezione di tutti i dati, in funzione del livello stesso di confidenzialità.

Nella tabella di seguito sono riportati i livelli definiti per la classificazione delle informazioni e dei documenti. Il livello di sicurezza richiesto attiene all'oggetto/contenuto dell'informazione e non alla modalità o supporto di formalizzazione.

Pertanto, anche per le informazioni non formalizzate in documenti, vale la classificazione indicata per quelle formalizzate.

Pubblico
Interno
Confidenziale
Strettamente Confidenziale

Sono considerate critiche tutte le informazioni contenute in documenti aziendali o di provenienza esterna la cui diffusione, dolosa o accidentale, potrebbe danneggiare gravemente gli interessi economici, finanziari e d'immagine. Tali informazioni dovranno essere protette e gestite con cautela, adottando misure che permettano la trasmissione sicura/cifrata tra punti di contatto reciprocamente validati e storage in ambienti protetti e crittografati. Di norma il trasferimento delle informazioni confidenziale deve avvenire tramite canali specifici dedicati e sicuri.

## 2.4 Utenze per l'erogazione e accesso al Servizio e alle Informazioni

Il Fornitore garantisce che tutte le risorse impiegate l'erogazione del servizio sono opportunamente formate e sensibilizzate sugli aspetti di sicurezza e tutela delle informazioni di *AULSS n. 9 Scaligera*, e che sono previsti internamente piani di formazione adeguati rispetto al mantenimento delle competenze e alle necessità di aggiornamento. Sono dunque previste, ove necessario, opportune sessioni di training specialistiche e focalizzate all'ambito operativo dei servizi erogati a favore di *AULSS n. 9 Scaligera*.

Tali sessioni dovranno prevedere anche le tematiche di Business Continuity del servizio, se applicabile.

Il Fornitore deve garantire la veridicità delle informazioni relative al riconoscimento dei propri dipendenti necessarie per l'accredito per l'accesso ai sistemi di *AULSS n. 9 Scaligera*. Tramite il Dipartimento IT di *AULSS n. 9 Scaligera*, se necessarie per lo svolgimento delle attività, saranno fornite le credenziali per accedere ai sistemi. Le utenze saranno nominali e dotate di opportuni profili.

Nel caso le risorse utilizzino credenziali per l'accesso ai sistemi di *AULSS n. 9 Scaligera* Il Fornitore è tenuto a segnalare tempestivamente (entro 24 ore) ogni situazione che comporti la variazione dei privilegi di accesso o la disattivazione dell'account dedicato. Qualsiasi ritardo di questa comunicazione, ritardo che possa comportare un rischio sulla gestione dei dati aziendali, potrà comportare una verifica di tipo Ispettivo e, in caso di accertate non conformità, un iter di violazione nei confronti del Fornitore.

È vietato utilizzare utenze personali assegnate da *AULSS n. 9 Scaligera* in sistemi di automazione che effettuino in modalità automatica serie di operazioni ripetitive normalmente eseguite da un operatore. Esigenze specifiche saranno valutate dal Dipartimento IT di *AULSS n. 9 Scaligera* e, se possibile, sarà creata e assegnata una nuova utenza appositamente definita con requisiti propri delle utenze di servizio. Qualsiasi utilizzo anomalo delle utenze personali saranno passibili di sospensione o revoca e di rivalsa da parte *AULSS n. 9 Scaligera* verso il Fornitore stesso.

## 2.5 Auditing Cybersecurity & Compliance

*AULSS n. 9 Scaligera*, essendo un Ente facente parte della Pubblica Amministrazione, ed operante nella Pubblica Sanità, è soggetta fortemente al rischio Cyber. Da qui la necessità che tutta l'organizzazione, comprese le filiere di approvvigionamento (Supply Chain), consideri con attenzione tutte le problematiche della sicurezza volte a proteggere i dati e gli asset.

*AULSS n. 9 Scaligera*, per accertare la compliance alle policy di sicurezza, potrà effettuare degli accertamenti ai servizi offerti dal Fornitore, essenzialmente con due modalità:



- Tramite la compilazione del questionario *Cybersecurity Questionnaire*;
- Con una Verifica ispettiva di Sicurezza (on-site).

Gli accertamenti riguarderanno esclusivamente il perimetro della soluzione e/o del servizio proposto e della tipologia di dati raccolti. Tali verifiche potranno essere estese ai requisiti richiesti per la Business Continuity del servizio, se applicabile.

Nel caso in cui *AULSS n. 9 Scaligera* dovesse identificare delle non conformità imputabili al Fornitore, sia a livello operativo sia a livello di requisiti, i costi derivanti per la risoluzione saranno completamente a carico del Fornitore. Nel caso in cui, invece, le non conformità siano dovute a modifica di normative o a nuovi requisiti espressi da *AULSS n. 9 Scaligera*, gli eventuali costi per la risoluzione saranno concordati tra le parti.

Qualora *AULSS n. 9 Scaligera*, a seguito dei risultati ottenuti dalle Verifiche Ispettive e/o a seguito dell'analisi della documentazione, rilevi delle "non conformità" o un livello inadeguato di sicurezza correlato al rischio identificato, il Fornitore si impegna a definire e condividere con *AULSS n. 9 Scaligera* un programma di miglioramento delle condizioni e delle contromisure adottate, dichiarando i tempi di implementazione e i benefici attesi.

Si precisa che nei casi più gravi dove, rispetto a quanto dichiarato dal Fornitore, le violazioni delle misure di sicurezza possano compromettere il business o la reputazione di *AULSS n. 9 Scaligera*, queste potrebbero costituire giusta causa per una immediata risoluzione contrattuale, salva ogni più ampia riserva di rivalsa legale.

## Modalità di verifica

In caso di fornitura di particolari servizi o applicativi, soprattutto nel caso vengano trattati dati personali, *AULSS n. 9 Scaligera* potrà richiedere al Fornitore la compilazione di un questionario di Cybersecurity. Nel rispondere al questionario, il Fornitore dovrà dichiarare di essere Conforme/Compliant, Parzialmente Conforme/Partially Compliant, o Non Conforme/Not Compliant ai requisiti indicati e alle applicazioni delle best practice internazionali, descrivendo lo stato dell'arte dei temi di sicurezza del servizio offerto.

I questionari saranno realizzati specificatamente per il servizio sottoposto a verifica e funzione del tipo di necessità di approfondimento.

Come linea guida per la realizzazione del questionario, *AULSS n. 9 Scaligera* fa riferimento al "Cybersecurity Framework", emesso dal NIST (National Institute of Standards e Technology).

Per il mercato italiano è disponibile il framework di riferimento reperibile al seguente link: [www.cybersecurityframework.it](http://www.cybersecurityframework.it) dove è possibile trovare le linee guida per la valutazione del rischio, i livelli di priorità per le implementazioni, la maturità del sistema e la lista dei controlli di Cybersecurity.

Il Fornitore è tenuto a rispondere alla compilazione del questionario entro 15 gg solari dalla richiesta di *AULSS n. 9 Scaligera* e si assumerà la responsabilità della veridicità dello stesso.

*AULSS n. 9 Scaligera* si riserva il diritto di procedere all'esecuzione di attività di auditing in ambito sicurezza e compliance on-site, per accertare che le misure adottate dal Fornitore per soddisfare i requisiti di sicurezza, siano conformi al dichiarato e assicurino un adeguato livello di sicurezza in tutti gli ambiti a cui l'ordine/contratto fa riferimento.

Prima di procedere alle verifiche, al Fornitore sarà dato un preavviso di cortesia di (almeno) 10 (dieci) giorni lavorativi, in forma scritta, fatto salvi i casi di incidenti gravi sul servizio erogato o le esigenze imposte da Autorità Giudiziaria, Garante della Privacy o Enti Governativi.

*AULSS n. 9 Scaligera* si riserva la possibilità di eseguire direttamente la verifica oppure di richiederne l'esecuzione ad una terza parte indipendente, qualificata e non concorrente con il Fornitore.

Le verifiche riguarderanno esclusivamente il perimetro della soluzione e/o del servizio proposto e dei dati raccolti. Tali verifiche potranno essere estese ai requisiti richiesti per la Business Continuity del servizio, se applicabile.

Il Fornitore accetta che *AULSS n. 9 Scaligera* possa richiedere evidenza del rispetto dei requisiti in riferimento alle attività svolte per *AULSS n. 9 Scaligera*. Di seguito alcuni esempi di verifiche che potrebbero essere richieste (se in ambito del servizio offerto):

- *evidenze della documentazione relativa all'organizzazione della sicurezza nella struttura organizzativa del Fornitore;*
- *evidenze delle attività di hardening, patching e upgrade dei sistemi operativi e degli applicativi usati per erogare il servizio a AULSS n. 9 Scaligera;*
- *evidenze della documentazione che descrive le procedure e le misure di sicurezza adottate per la protezione fisica e per la regolamentazione degli accessi alle sale dati ed ai locali ove sono svolte le attività erogate o conservati dati di AULSS n. 9 Scaligera*
- *Se in ambito, al servizio erogato, evidenze della documentazione delle procedure di Business Continuity implementate presso le sedi del Fornitore*

- *Evidenze delle misure atte a mitigare il rischio Cyber sulle attività o soluzioni svolte per AULSS n. 9 Scaligera.*
- *L'organizzazione delle attività previste per le verifiche sarà mutualmente definita e concordata tra le parti, evitando di interferire con le normali attività di business.*

Il Fornitore si impegna, inoltre, ad offrire ogni supporto necessario a tali attività di verifica, rispondendo alle richieste di informazioni e chiarimenti e fornendo la documentazione eventualmente richiesta.

*AULSS n. 9 Scaligera* o la società incaricata eseguirà o farà eseguire detta verifica ispettiva senza che ciò determini una disclosure e/o altra violazione di qualsiasi diritto di proprietà intellettuale del Fornitore, che dovranno essere in ogni caso tutelati e protetti: compatibilmente a detti diritti sarà svolta l'ispezione.

## 2.6 Incident e Data Breach Management

Il Fornitore deve garantire l'esercizio di un processo di raccolta e segnalazione degli incidenti di sicurezza, anche nel caso di ausilio di eventuali Terze Parti esterne, in modo da garantire che gli eventi anomali/incidenti, che possono avere ripercussioni sui sistemi, sulle reti e sulle informazioni gestite in perimetro dei servizi erogati per *AULSS n. 9 Scaligera* o con impatto su di essi, siano tempestivamente riconosciuti e adeguatamente gestiti mediante l'utilizzo di efficienti sistemi di analisi, comunicazione e reazione.

È richiesto da *AULSS n. 9 Scaligera* una accurata attenzione al rilevamento di eventi che possano comportare anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati (anche personali) trasmessi, memorizzati o comunque elaborati, nonché la violazione o l'intrusione di parti dell'infrastruttura ICT di *AULSS n. 9 Scaligera* (c.d. "Supply Chain attacks").

Il processo di gestione degli incidenti deve prevedere le seguenti fasi:

- L'identificazione tempestiva di eventuali violazioni;
- Raccolta delle informazioni delle violazioni;
- Valutazione del rischio e individuazione del tipo di incidente (esempio se riguarda dati personali);
- Individuazione del riferimento aziendale per la gestione dell'incidente;
- Definizione del piano di comunicazione e di condivisione con *AULSS n. 9 Scaligera*.

Queste fasi devono essere adeguatamente predisposte in base ad un idoneo piano di gestione delle violazioni fondato su un'accurata analisi del rischio, in modo da ridurre al minimo il livello di arbitrarietà e discrezionalità nella gestione degli incidenti.

Il Fornitore si impegna a rispondere con la massima celerità agli incidenti di sicurezza rilevati e a risolverli in maniera rapida, formale ed efficace al fine di attenuarne gli effetti per *AULSS n. 9 Scaligera*.

### 2.6.1 Incidenti Cyber

Nel caso in cui sistemi o apparati sotto il controllo del Fornitore siano sotto una minaccia di tipo Cyber e vi sia la possibilità che tale minaccia si propaghi ai sistemi, alle reti o agli apparati di *AULSS n. 9 Scaligera*, deve essere effettuata una segnalazione tempestiva e comunque entro al massimo 24 ore solari dal momento in cui il Fornitore è venuto a conoscenza dell'incidente.

La segnalazione per iscritto deve essere inviata all'indirizzo di posta di XYXYXYX:  
\_\_\_\_\_@\_\_\_\_\_

La segnalazione dovrà contenere, oltre a un punto di contatto di chi si occupa dell'emergenza da parte del Fornitore, tutte le informazioni relative agli *Indicatori di Compromissione* tra cui, ad esempio, domini, url, ip, hash, md5, i sistemi e i dati potenzialmente violati e, in generale, le informazioni sul tipo di minacce e vulnerabilità e i sistemi/reti di *AULSS n. 9 Scaligera* potenzialmente coinvolti dalla minaccia.

Queste informazioni sono un elemento essenziale per *AULSS n. 9 Scaligera* al fine di poter valutare in modo organico e analitico le proporzioni dell'incidente stesso da cui eventualmente far partire le azioni di mitigazione e protezione.

Nel caso in cui sia presente una violazione dei dati, intesa come accesso non autorizzato al contenuto, i dati possono essere classificati come:

- violazione dati personali (Data Breach);
- violazione dati di business di *AULSS n. 9 Scaligera*.

Nella segnalazione al CISO/RESPONSABILE IT /DIPARTIMENTO IT /XXXXX di *AULSS n. 9 Scaligera* deve essere indicato anche il tipo di dati che, anche solo potenzialmente, si ritenga possano essere stati compromessi.

Nel caso in cui siano violati dati personali di qualsiasi genere, il Fornitore dovrà effettuare una ulteriore comunicazione come indicato al punto successivo.

Nel caso il servizio sia in ambito Business Continuity dovranno essere applicate anche le modalità di comunicazione previste nel BCP (Business Continuity Plan).

## 2.6.2 Incidenti di sicurezza con Data Breach

Con il termine *data breach* si intende un incidente di sicurezza in cui dati personali o particolari/sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

L'art. 33 del Regolamento 2016/679 impone al titolare di notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il titolare acquisisce consapevolezza dell'avvenuta violazione.

In considerazione di quanto descritto, gli incidenti in ambito data breach devono essere comunicati tempestivamente a *AULSS n. 9 Scaligera* all'indirizzo di posta elettronica: \_\_\_\_\_@\_\_\_\_\_

Per i dettagli sulla comunicazione e sulle tempistiche richieste da *AULSS n. 9 Scaligera* ai Fornitori, si fa riferimento alle istruzioni operative contenute nelle Nomine a Responsabile al Trattamento dei Dati Personali.

### 3 Regole di Data Protection

È sempre richiesto siano garantite per i dati la riservatezza, l'integrità e disponibilità, attraverso l'adozione di misure di sicurezza che riguardano tra le altre, la protezione fisica dei dispositivi, le procedure di accesso ai sistemi.

Di seguito le indicazioni relative a:

- Il Trattamento dei Dati;
- Gestione degli Amministratori di Sistema (AdS)
- Gestione della conservazione e cancellazione dei dati;
- Sistemi del Fornitore per il trattamento di dati;
- Protezione delle aree di lavoro;
- Requisiti minimi per la protezione degli strumenti di lavoro elettronici;
- Accesso da remoto ai dati e alle applicazioni.

#### 3.1 Il Trattamento dei Dati

Nell'ambito dei processi che coinvolgono la data protection son stati individuate 3 classi nelle quali si distinguono i dati:

<i>Dati Impersonali e/o di Business (quindi confidenziali AULSS n. 9 Scaligera)</i>	<p>Sono considerati dati Impersonali e/o di Business i dati che, seppur non riconducibili a persone fisiche già tutelate dalle regole di Privacy, sono di rilievo per le attività d'impresa. La perdita o la diffusione illecita di queste informazioni potrebbe arrecare un danno commerciale, di posizionamento o di immagine con impatti economici potenzialmente molto rilevanti.</p> <p>Nel caso di presenza di dati Impersonali e/o di Business occorre prestare la massima attenzione per la salvaguardia dei dati aziendali che, seppur non soggetti alle regole del GDPR, rivestono molta importanza per il business dell'azienda.</p> <p>Il Fornitore deve garantire di mettere in atto tutte le azioni atte a ridurre al minimo il rischio residuo di violazione prestando la massima attenzione affinché i dati aziendali siano protetti adeguatamente in funzione anche della riservatezza del dato contenuto</p>
<i>Dati Personali Identificativi (anche dati di traffico)</i>	<p>Sono considerati Dati Personali identificativi i dati che permettono l'identificazione diretta, come i dati anagrafici (ad esempio: nome e cognome, codice fiscale) le immagini, numeri di telefono, indirizzi IP etc. Sono considerati Dati Personali Identificativi anche i dati di traffico telefonico.</p> <p>Il Fornitore, nel caso di presenza di Dati Personali, è obbligato a sottoscrivere l'atto di Nomina a Responsabile al Trattamento dei Dati Personali, come previsto dal contratto tra le parti.</p> <p>Nel caso di dati di Traffico l'accesso ai dati deve essere consentito attraverso accessi in strong authentication: si rimanda a requisiti tecnici funzionali forniti in sede di progetto</p>
<i>Dati Personali Particolari (rif Regolamento UE 2016/679 articolo 9)</i>	<p>I Dati Particolari sono i dati personali che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.</p> <p>I Dati Giudiziari sono i dati personali che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.</p> <p>I dati Particolari/Giudiziari richiedono specifiche autorizzazioni e modalità di accesso al dato come l'accesso tramite strong authentication, ovvero una autenticazione a due fattori, e un elenco ben definito di chi è abilitato ad accedere a questi dati.</p> <p>Nel caso di dati Particolari/Giudiziari saranno forniti requisiti dedicati e forniti in aggiunta a quanto descritto in questo documento e, quindi, si rimanda a requisiti tecnici funzionali forniti in sede di progetto</p>

### 3.2 Gestione degli Amministratori di Sistema

Per gli Amministratori di Sistema (AdS), sia che essi trattino dati personali o meno, dovranno aver ricevuto regole ed istruzioni contestualmente nell'atto di nomina che *il Fornitore avrà provveduto a far sottoscrivere ai propri AdS*, così come anche previsto nel documento di nomina del Responsabile Esterno al Trattamento ricevuto da parte *AULSS n. 9 Scaligera* in qualità di Titolare al Trattamento per il contratto oggetto del presente Addendum.

### 3.3 Gestione della conservazione e cancellazione dei dati

I tempi di retention dei dati di *AULSS n. 9 Scaligera* necessari per compiere le attività devono rispettare i valori concordati con *AULSS n. 9 Scaligera*.

Il tempo massimo di archiviazione dei dati trattati dal Fornitore deve essere commisurato in base alla normativa vigente.

Nel Regolamento Privacy Europeo 679/2016 è stato rafforzato il diritto alla cancellazione dei Dati Personali (right to be forgotten) nell'articolo 17. In base ad esso l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nei seguenti casi:

- I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- I dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- I dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.
- I dati personali sono stati trattati illecitamente;
- L'interessato revoca il consenso su cui si basa il trattamento, se non esiste alcun altro motivo legittimo per il trattamento;
- L'interessato si oppone al trattamento e non sussiste alcun ulteriore motivo legittimo per procedere il trattamento;

*AULSS n. 9 Scaligera*, in quanto titolare del trattamento nei casi indicati, è obbligato a procedere alla cancellazione dei dati e adottare misure ragionevoli per informare altri titolari del trattamento che stanno trattando i dati, compreso qualsiasi link, copia o riproduzione, di procedere alla cancellazione.

Il Fornitore, se detiene dati di cui *AULSS n. 9 Scaligera* è Titolare, deve quindi garantire adeguate misure e strumenti affinché l'operazione di cancellazione richiesta da *AULSS n. 9 Scaligera* sia possibile, rapida ed efficace.

### 3.4 Sistemi del Fornitore per il trattamento di dati

Nel caso per la tipologia di servizio offerto presso proprie sedi/spazi, il Fornitore necessita di utilizzare software e/o sistemi applicativi non governati da *AULSS n. 9 Scaligera* per la gestione di dati di proprietà, titolarità o comunque riferiti a *AULSS n. 9 Scaligera*, è tenuto a informare *AULSS n. 9 Scaligera*.

Il Fornitore sarà in ogni caso responsabile della conformità, l'integrità, la disponibilità e la riservatezza dei dati trattati. Il Fornitore deve quindi garantire che il software utilizzato sia conforme ai requisiti minimi di Cybersecurity, secondo la normativa vigente e le Best Practice internazionali.

*AULSS n. 9 Scaligera* si riserva la possibilità di richiedere la compilazione di un Cybersecurity Questionnaire (allegato al presente Addendum) tramite il quale il Fornitore dichiarerà la propria compliance ai requisiti di sicurezza.

*AULSS n. 9 Scaligera* si riserva, nel caso in cui il Fornitore tratti rilevanti quantità di dati sui propri sistemi, la possibilità di effettuare dei test di sicurezza sui sistemi, a proprie spese e senza oneri per il Fornitore, dando un preavviso minimo di 10 giorni solari in forma scritta. Le attività previste per le verifiche saranno mutualmente definite e concordate tra le parti, evitando di interferire con le normali attività di business e senza causare violazione di qualsiasi diritto di proprietà intellettuale del Fornitore.

Nel caso siano trattati dati di Clienti di *AULSS n. 9 Scaligera*, il Fornitore deve verificare siano applicati e implementati nei propri software misure di sicurezza idonee alla protezione e in linea con quanto previsto dal presente Addendum, dalle politiche definite da *AULSS n. 9 Scaligera*, e conformi alle normative cogenti, così come previsto nel Par. 6 e successivi. In alternativa possono essere utilizzate analoghe misure di sicurezza, sempre garantendo come minimo il medesimo livello di sicurezza.

### 3.5 Protezione delle aree di lavoro

Anche nel caso in cui il servizio oggetto del presente Addendum sia erogato presso sedi diverse da quelle di *AULSS n. 9 Scaligera*, dovranno essere adottate misure di sicurezza idonee alla tipologia di dati trattati e adeguate a preservare confidenzialità, integrità e disponibilità delle informazioni.

Pertanto, il Fornitore anche presso proprie sedi/spazi, garantisce un'adeguata protezione fisica dei locali contenenti il personale, apparati e dispositivi abilitati a gestire informazioni, a trattare dati o accedere ai sistemi di *AULSS n. 9 Scaligera*.

Le seguenti misure, e regole richieste prevedono:

- il *perimetro di sicurezza* delle zone ove i dati sono memorizzati o trattati, deve essere definito chiaramente, dotato di un adeguato sistema di controllo accessi per verificare che l'accesso sia permesso alle sole persone autorizzate, con memorizzazione degli accessi e delle uscite; inoltre, il perimetro deve essere adeguatamente protetto contro le intrusioni dall'esterno, nonché dotato di sistemi antintrusione automatica, con memorizzazione degli allarmi rilevati;
- i *sistemi di videosorveglianza* devono permettere di tenere sotto controllo ogni parte del perimetro della zona da proteggere ed in particolare i punti di passaggio più significativi: a tale scopo l'illuminazione deve essere adeguata; i sistemi di videosorveglianza devono essere conformi al Provvedimento dell'Autorità Garante per la Privacy dell'08 aprile 2010;
- il personale appartenente a funzioni non direttamente connesse con la gestione operativa diretta di quanto contenuto nelle aree protette e le apparecchiature non direttamente connesse a tali fini (per esempio fotocopiatrici e fax) devono essere situate all'esterno delle aree protette
- l'autorizzazione all'ingresso in aree protette di detto personale deve essere gestita dal Responsabile delle infrastrutture, d'intesa con il Responsabile della Sicurezza fisica aziendale;
- negli uffici o altri ambienti preposti devono essere garantite le normative generali di sicurezza Fisica e disporre di un adeguato sistema di alimentazione tramite UPS.

Nel caso in cui il servizio del Fornitore preveda attività al di fuori delle proprie sedi/spazi, come per esempio attività di reperibilità notturna/festiva o smartworking, tale attività dovrà essere comunicata a *AULSS n. 9 Scaligera* in fase di definizione del contratto.

Il Fornitore si impegna a istruire il proprio personale a adottare tutte le misure minime idonee a garantire la riservatezza delle informazioni anche in luoghi diversi delle proprie sedi.

### 3.6 Requisiti minimi per la protezione degli strumenti di lavoro elettronici

Nel presente capitolo sono indicati i requisiti minimi per la sicurezza dei dispositivi elettronici utilizzati dal Fornitore, anche nel caso lo stesso utilizzo sistemi propri nel trattamento di date di *AULSS n. 9 Scaligera*.

Tali misure e le relative procedure, sono richieste in quanto nel corso dei trattamenti, ed erogazione dei servizi, si potrebbero provocare incidenti che comporterebbero notevoli danni con impatti non solo sugli aspetti di sicurezza delle informazioni, ma anche di Business, legali e d'immagine a *AULSS n. 9 Scaligera* e al Fornitore stesso.

I Fornitori e i loro dipendenti sono responsabili della protezione dei dati presenti sui propri dispositivi aziendali, e sono responsabili di garantire la protezione dei dispositivi e dei supporti di archiviazione utilizzati per accedere, elaborare o archiviare i dati utilizzati per condurre attività lavorativa con *AULSS n. 9 Scaligera* o interagire con le reti esterne e i sistemi aziendali di *AULSS n. 9 Scaligera*, siano essi di proprietà o affittati da *AULSS n. 9 Scaligera*, dal dipendente o da terze parti. In caso di smarrimento o furto di un dispositivo o di un supporto di archiviazione, è necessario segnalarlo prontamente all'organo aziendale competente.

I Fornitori e i loro dipendenti possono utilizzare sui propri dispositivi aziendali i dati riservati di cui *AULSS n. 9 Scaligera* è Titolare (personali e/o di business) solo se autorizzati. A tale scopo si potranno utilizzare solo i dati essenziali, necessari e pertinenti, per raggiungere le finalità richieste dal trattamento.

REQUISITI MINIMI DI SICUREZZA	
STRUMENTI ELETTRONICI (laptop, notebook, etc)	MISURE DA ADOTTARE <ul style="list-style-type: none"><li>● Gestione dei diritti di amministratore</li><li>● Definizione e implementazione di un set minimo di software a garanzia della protezione (antivirus, antimalware, local firewall, etc.)</li><li>● Aggiornamento del SO all'ultima patch di sicurezza disponibile</li><li>● Adozione di funzionalità di protezione dei dati e di crittografia della memoria (es. Bitlocker)</li><li>● Utilizzo dello screen saver con accesso mediante password attivabile direttamente dall'utente, o con blocco automatico dopo un tempo minimo predefinito di inattività</li><li>● Utilizzo di ID e password personali all'apparato assegnato</li></ul>

	<p>ATTIVITA' PROIBITE</p> <ul style="list-style-type: none"> <li>● Trattamento di dati personali o aziendali di proprietà di <i>AULSS n. 9 Scaligera</i> per motivi diversi da quello relativo al contratto oggetto dell'Addendum</li> <li>● Estrazione / copia, di dati anche tramite funzionalità ammesse dal profilo di abilitazione assegnato, in dispositivi che non siano dispositivi di proprietà del Fornitore e autorizzati da <i>AULSS n. 9 Scaligera</i></li> </ul>
POSTA ELETTRONICA	<p>MISURE DA ADOTTARE</p> <ul style="list-style-type: none"> <li>● siano previste misure antispam e anti-malware a protezione della posta elettronica;</li> <li>● sia presente un sistema di protezione da contenuti non autorizzati (Content Filtering), che provveda al blocco di talune tipologie di file allegati e/o altri elementi o programmi contenuti nel messaggio di posta elettronica;</li> </ul> <p>ATTIVITA' PROIBITE</p> <ul style="list-style-type: none"> <li>● - uso dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum, mailing-list, ecc., salvo diversa ed esplicita autorizzazione;</li> <li>● - uso in modo non autorizzato, o contraffazione, delle informazioni di intestazione delle e-mail;</li> <li>● - invio di informazioni societarie attraverso account personali di posta elettronica (anche nel caso in cui ci si trovi lontani dalla propria sede di lavoro);</li> <li>● - diffusione di informazioni aziendali non "pubbliche" a persone che non appartengono a elenchi di indirizzi e-mail <i>AULSS n. 9 Scaligera</i>, senza preventiva autorizzazione.</li> <li>● Invio di dati personali o aziendali di proprietà di <i>AULSS n. 9 Scaligera</i> per motivi diversi da quello relativo al contratto oggetto dell'Addendum</li> </ul>
SERVER	<p>MISURE DA ADOTTARE</p> <ul style="list-style-type: none"> <li>● Gestione dei diritti di amministratore</li> <li>● Definizione e implementazione di un set minimo di software a garanzia della protezione (antivirus, antimalware, local firewall, etc.)</li> <li>● Aggiornamento del SO all'ultima patch di sicurezza disponibile</li> <li>● Utilizzo di ID e password personali e dedicate all'apparato assegnato</li> </ul> <p>ATTIVITA' PROIBITE</p> <ul style="list-style-type: none"> <li>● Trattamento di dati personali o aziendali di proprietà di <i>AULSS n. 9 Scaligera</i> per motivi diversi da quello relativo al contratto oggetto dell'Addendum</li> <li>● Estrazione / copia, di dati anche tramite funzionalità ammesse dal profilo di abilitazione assegnato, in dispositivi che non siano dispositivi di proprietà del Fornitore e autorizzati da <i>AULSS n. 9 Scaligera</i></li> </ul>

**In merito alle attività effettuate tramite apparati (PC o altro) connessi alla rete *AULSS n. 9 Scaligera* o ai sistemi *AULSS n. 9 Scaligera*, le attività seguenti devono essere proibite, salvo eccezioni autorizzate da *AULSS n. 9 Scaligera* su uno specifico perimetro in quanto legate ad es. alle attività oggetto di servizio: scansione della rete, fingerprinting dei servizi, tentativi di VA/PT, attacchi DoS o comunque volti a causare indisponibilità di risorse, ed in generale attività di hacking/ethical hacking se non espressamente autorizzata;**

È altresì richiesto:

- di adottare una modalità "clear desk" per ridurre il rischio di accessi non autorizzati, o danni, alle informazioni su supporto cartaceo tramite l'impiego di cassette e armadi con chiave;
- la trasmissione all'esterno di documenti classificati come Confidenziale o Strettamente Confidenziale devono seguire le indicazioni indicate da *AULSS n. 9 Scaligera*. In ogni caso la trasmissione delle informazioni classificate deve avvenire in modalità sicura e cifrata.



### 3.7 Accesso da remoto ai dati e alle applicazioni

Quando previsto *AULSS n. 9 Scaligera* fornirà specifiche credenziali di accesso remoto al perimetro fisico anche dall'esterno, attraverso connessione VPN, che dovranno essere utilizzate unicamente previo autorizzazione.

Le credenziali saranno assegnate individualmente / nominalmente, adottando il principio di necessità nella definizione dei profili. Il Fornitore dovrà garantire il rispetto di tali procedure, affinché ai dati possa accedere unicamente chi direttamente incaricato, nel rispetto della massima riservatezza.

Le credenziali sono personali e riservate e dovranno essere custodite con le necessarie cautele evitandone la condivisione.

È responsabilità del Fornitore e del dipendente del Fornitore stesso che esegue il collegamento remoto assicurarsi che non vengano realizzati accessi non autorizzati e potenzialmente dannosi a risorse o informazioni aziendali.

ACCESSO REMOTO (VPN)	ATTIVITA' PROIBITE
	<ul style="list-style-type: none"><li>● Accedere da remoto alla rete o applicativi <i>AULSS n. 9 Scaligera</i> senza essere stati autorizzati a farlo o con modalità diverse da quelle indicate/permesse;</li><li>● Mantenere il proprio dispositivo connesso contemporaneamente a rete/VPN <i>AULSS n. 9 Scaligera</i> e altre VPN, salvo esplicita autorizzazione scritta;</li><li>● Utilizzare credenziali di cui non si è l'assegnatario o permettere ad altri di usufruire delle proprie;</li><li>● Eseguire connessioni remote anche tramite VPN alla rete interna <i>AULSS n. 9 Scaligera</i> da computer non aziendali salvo esplicita autorizzazione scritta;</li><li>● Accedere remotamente dalla rete <i>AULSS n. 9 Scaligera</i>, salvo autorizzazione, a computer/dispositivi posti all'esterno di essa;</li><li>● Utilizzare dispositivi informatici privati dei dipendenti non assegnati dal Fornitore;</li><li>● Utilizzare strumenti di condivisione della connessione o del dispositivo.</li></ul>

I dispositivi utilizzati devono essere conformi a quanto espressamente indicato nel precedente paragrafo 3.6

Inoltre, è assolutamente vietato l'utilizzo di strumenti informatici o multimediali che permettano la condivisione del dispositivo connesso alla rete di *AULSS n. 9 Scaligera*. Ad esempio, quando si accede agli applicativi *AULSS n. 9 Scaligera*, sono assolutamente vietati l'utilizzo di programmi o applicazioni che permettano la condivisione dello schermo del dispositivo connesso o strumenti che permettano il controllo del dispositivo connesso alla rete *AULSS n. 9 Scaligera* da personale remoto. In ogni caso è vietato il trasferimento a terzi dei contenuti che emergono da sessioni di condivisione fra *AULSS n. 9 Scaligera* e il Fornitore.

Si precisa che nei casi più gravi queste violazioni delle misure di sicurezza potrebbero compromettere il business o la reputazione di *AULSS n. 9 Scaligera*, oltre che a possibili accessi non autorizzati a dati personali e/o di business con conseguente apertura di procedura di infrazione da parte degli Organi Governativi competenti. Nel caso di accertamento di violazioni, queste potrebbero costituire giusta causa per una immediata risoluzione contrattuale con il Fornitore, salva ogni più ampia riserva di rivalsa legale.

#### 3.7.1 Accesso da paesi extra EU

Se già non precedentemente normato tra le parti in fase di stipula del contratto, qualora il Fornitore debba consentire l'accesso ai propri sistemi dove siano contenuti dati personali di *AULSS n. 9 Scaligera* da luoghi Extra EU, ad esempio per attività di esercizio o manutenzione anche a carattere straordinario, è obbligato ad informare preliminarmente *AULSS n. 9 Scaligera*, anche nel corso della durata del contratto. Tale obbligo vale anche nel caso in cui non sia previsto un trattamento di dati personali, disciplinato dal GDPR.

Il Fornitore ha l'obbligo di cooperare con *AULSS n. 9 Scaligera* per valutare se il Paese Terzo oggetto di trasferimento dei dati personali garantisce un livello di protezione sostanzialmente equivalente a quello previsto dal GDPR e, se del caso, adottare ulteriori misure addizionali volte a garantire tale livello di adeguatezza.

Le parti si impegnano altresì a disciplinare tale trasferimento in maniera adeguata e conforme a quanto previsto dal capo V del GDPR.

Anche l'utilizzo di strumenti virtuali come, ad esempio, Virtual Desktop Infrastructure (VDI) ovvero una tecnologia di virtualizzazione che ospita un sistema operativo desktop e le applicazioni su un server centralizzato



in un centro dati, se questo server è posizionato al di fuori della Unione Europea deve essere preventivamente effettuata una valutazione congiunta tra le aree competenti del Fornitore e di *AULSS n. 9 Scaligera*.

### 3.7.2 Smart Working e attività in Reperibilità

Il Fornitore è tenuto a garantire di formare e informare i propri dipendenti sui temi di Sicurezza Informatica che riguardino lo Smartworking, e/o le attività svolte in orario di Reperibilità quando previsto, in rispetto delle misure di protezione dei dati nei luoghi di lavoro pubblici e privati.

Infatti, oltre a tutte le regole normalmente applicate nei luoghi di lavoro appropriati, si aggiungono regole di privacy e confidenzialità relative ai luoghi dove il personale svolge l'attività lavorativa da remoto.

SMART WORKING	<b>MISURE DA ADOTTARE</b> <ul style="list-style-type: none"><li>● utilizzo solo strumenti aziendali regolarmente assegnati dal Fornitore;</li><li>● porre attenzione ad accessi non autorizzati ai dispositivi (ad esempio da parte di membri della propria famiglia);</li><li>● non concedere l'utilizzo, anche temporaneo dei dispositivi assegnati;</li><li>● adottare tutte le precauzioni per garantire la confidenzialità delle informazioni (ad esempio lo schermo non sia consultabile da terzi);</li><li>● adottare tutte le precauzioni per evitare che meeting e conversazioni possano essere ascoltate da terzi;</li><li>● non lasciare contratti o documenti incustoditi in posizioni accessibili da terzi;</li><li>● adottare tutte le cautele per evitare la sottrazione del dispositivo utilizzato e, nel caso di perdita, avvisare immediatamente il proprio Help Desk per attivare le contromisure previste;</li><li>● utilizzare solo connessioni sicure evitando gli accessi pubblici e/o utilizzare solo connessioni in VPN</li></ul>
---------------	--

Il Fornitore sarà responsabile di tutte le attività svolte dal proprio personale, anche durante le attività di smart working, del verificarsi di incidenti di sicurezza derivanti dall'adozione scorretta della modalità di utilizzo

## 4 Supply Chain Security

Per Supply Chain Security si intende il processo e le misure di sicurezza adottate che permettono di portare un prodotto trasferendolo dalla sede Fornitore fino a una o più sedi definite dal contratto tra le parti in modo sicuro. Tali misure si applicano anche in tutti i casi di trasporto di materiali *AULSS n. 9 Scaligera* sotto la responsabilità del Fornitore.

Nel caso in cui sia prevista la fornitura di materiali informatici (hardware e software), il Fornitore è tenuto a verificare la catena di approvvigionamento con una valutazione e analisi dei rischi, mitigarne gli effetti e costruire una valida resilienza. Devono essere adottate adeguate misure di sicurezza per prevenire la compromissione del Software o hardware e/o l'accesso non autorizzato durante tutte le fasi di trasporto.

Le informazioni di configurazione o i dati personali non devono essere contenuti nei dispositivi durante il trasporto. Per le attività di manutenzione e riparazione dei dispositivi che prevedono il trasferimento dell'hardware (dal sito del cliente a quello del fornitore o tra diversi siti gestiti da *AULSS n. 9 Scaligera*) i dispositivi devono essere protetti, possibilmente inizializzati e senza dati memorizzati, al fine di evitare possibili manomissioni dei dispositivi stessi durante le fasi di trasporto. Nel caso di dispositivi contenenti rilevanti quantitativi di dati, come ad esempio il trasferimento di sede di un Server configurato o di una unità di Storage, le modalità di trasporto sicuro dovranno essere valutate congiuntamente con il Responsabile IT / CISO di *AULSS n. 9 Scaligera* in accordo con le policy interne.

Su richiesta di *AULSS n. 9 Scaligera* il Fornitore è tenuto a redigere un piano di sicurezza della supply chain con la descrizione con i dettagli delle misure di sicurezza legate alla fornitura e l'eventuale installazione in opera. Il piano di sicurezza della supply chain consentirà a *AULSS n. 9 Scaligera* di valutare l'ambiente di sicurezza in cui opera il proprio Fornitore e di verificare se siano adottate adeguate misure di sicurezza.

Le misure di sicurezza dovranno riguardare gli asset, il personale, le informazioni, la sicurezza delle merci e dei trasporti.

Per referenze e informazioni sulla Supply Chain Security si consulti le indicazioni del NIST:

<https://csrc.nist.gov/projects/supply-chain-risk-managements>

[https://www.nist.gov/sites/default/files/documents/itl/csd/NIST\\_USRP-Cisco-Cyber-SCRM-Case-Study.pdf](https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Cisco-Cyber-SCRM-Case-Study.pdf)

## Requisiti per fornitura, integrazione o lo sviluppo di applicativi software firmware e/o sistemi

Di seguito sono contenuti i requisiti di sicurezza base richiesti al Fornitore per le attività di:

- Fornitura di Software, anche come rivendita e integrazione e configurazione,
- Fornitura di un dispositivo con relativo firmware, di un sistema informatico
- Sviluppo di software dedicato per *AULSS n. 9 Scaligera*.
- Sviluppo di un applicativo per *AULSS n. 9 Scaligera*,

L'applicativo/tool/sistema dovrà rispettare quanto previsto in fase di progetto e le misure di sicurezza descritte in questo documento, ove e se applicabili. Se necessario e se evidenziato in fase di progetto, potrà essere redatto un nuovo documento di sicurezza con la descrizione di ulteriori requisiti di dettaglio, specifico per tipo di servizio offerto. Il Fornitore avrà l'obbligo di adottare tutti i requisiti descritti.

*AULSS n. 9 Scaligera* non obbliga la scelta di una particolare soluzione tecnica ma, tramite emissione di requisiti di base, lascia al Fornitore la scelta tecnica e specifica dei meccanismi di sicurezza da implementare, in funzione delle esigenze e delle caratteristiche del servizio.

Al Fornitore quindi, in accordo con *AULSS n. 9 Scaligera*, spetta il compito di individuare i meccanismi di sicurezza da implementare, in considerazione del tipo di esposizione ai rischi, fisico o Cyber, della criticità a livello di business e della tipologia d'informazioni scambiate. Di tali meccanismi si darà opportuna evidenza a *AULSS n. 9 Scaligera* in sede di sviluppo di progetto, comunque preliminarmente all'accettazione positiva della fornitura da parte di *AULSS n. 9 Scaligera*.

Si sottolinea l'obbligo da parte del Fornitore di garantire in ogni caso la *totale conformità* dei software/sistemi secondo la normativa vigente e le Best Practice internazionali.

I requisiti descritti nei capitoli indicati si riferiscono principalmente a:

- Authentication, Authorization e Accounting;
- Posizionamento, Storage, Retention e Cancellazione dei dati;
- Tracciamento degli accessi e delle operazioni;
- Affidabilità, backup e amministratori di sistema
- Esposizioni delle interfacce su Intranet/Internet
- Secure Data Transfert
- Cifratura dei dati
- Sicurezza dell'infrastruttura
- Regole per lo sviluppo del codice
- Norme per l'utilizzo del Cloud
- Applicativi posizionati entro o al di fuori del perimetro di *AULSS n. 9 Scaligera*
- Aggiornamento del prodotto software
- Applicativo utilizzato da cliente *AULSS n. 9 Scaligera*
- Test di sicurezza

Nel caso in cui il servizio/applicativo/tool entri nel perimetro della Business Continuity di *AULSS n. 9 Scaligera*, il Fornitore è tenuto a:

- prendere visione dei livelli indicati e concordati in fase di definizione contratto;
- garantire i livelli indicati di ripristino del servizio, sia in termini di RTO, RPO e MBCO;
- formalizzare il BCP entro 30 giorni solari dall'erogazione del servizio;
- segnalare qualsiasi anomalia e/o impedimento che possano, anche temporaneamente, invalidare o compromettere il rispetto di tali tempi.

Nel caso in cui, data la complessità o particolarità del software offerto, dovessero essere necessari requisiti integrativi di sicurezza, come ad esempio, accorgimenti particolari e specifici inerenti al progetto, si precisa che questi requisiti saranno definiti in un addendum di sicurezza informatica appositamente scritto e allegato all'ordine/contratto. In caso deroghe o modifiche ai requisiti di sicurezza proposti, tali misure dovranno essere verificate congiuntamente con *AULSS n. 9 Scaligera* e in ogni caso garantire un livello di sicurezza non inferiore alle soluzioni consigliate da *AULSS n. 9 Scaligera*.

Il Fornitore, infine, dovrà descrivere nel dettaglio le soluzioni tecniche utilizzate (dispositivi hardware software impiegato, modalità operative, politiche di sicurezza, etc.) per la conformità ai requisiti di sicurezza.

Nel caso in cui il Fornitore non applichi i requisiti "in scope" alla fornitura, tale motivo potrà essere utilizzato come non conformità alle specifiche di progetto; l'inadempimento o parziale adempimento e comportare una azione legale e di rivalsa da parte di *AULSS n. 9 Scaligera*.

Nei successivi paragrafi, sono indicati i requisiti di base per i software oggetto di fornitura a *AULSS n. 9 Scaligera*, basati soprattutto sul controllo degli accessi, la protezione del dato e la connessione con software esterni. Tale elenco rappresenta un livello minimo di protezione e controllo e la necessità di integrazione/modifica dei requisiti deve essere concordato con il CISO/RESPONSABILE IT /DIPARTIMENTO IT /XXXXX .

## 5 Fornitura della componente Software

Tutti i software/firmware forniti devono essere sottoposti a verifica di sicurezza e alle disposizioni presenti in questo allegato. Anche i firmware presenti nei dispositivi, ovvero software specifici di base installati negli apparati, specie se connessi alla rete e dotati di shell o modalità di connessione da remoto (shell o interfacce alla rete di management) sono inclusi nelle disposizioni di sicurezza.

Possiamo avere due modalità:

- Progetto per fornitura in un applicativo (custom o anche la sola integrazione di un software commerciale);
- Fornitura di apparati con firmware interno (es. dispositivi di rete).

TIPOLOGIE SOFTWARE	DI	Software (o firmware) <i>sviluppato per conto di AULSS n. 9 Scaligera</i> ; AULSS n. 9 Scaligera affida lo sviluppo del software (sia esso ex novo o modifica di software esistente) a un fornitore e quest'ultimo si impegna a consegnare a AULSS n. 9 Scaligera il software sviluppato sulla base dei requisiti da questa definiti.
		Riutilizzo di software (o firmware) o parti di esso sviluppati per conto di AULSS n. 9 Scaligera: Software già esistente e disponibile
		Software (o firmware) <i>libero o a codice sorgente aperto</i> : o software con licenza Open Source. In particolare, si intende tutto il software distribuito sotto una <i>licenza certificata da OSI</i>
		Software fruibile in modalità cloud computing: FW acquisisce il software come servizio. In questa soluzione non sono ricomprese le soluzioni HaaS (Hardware as a Service) e IaaS (Infrastructure as a Service)
		Software (o firmware) di tipo proprietario mediante ricorso a licenza d'uso: software soggetto a condizioni di licenza d'uso di tipo proprietario da installare «on premise».
		Software (o firmware) <i>combinazione delle precedenti soluzioni</i> .

In funzione del tipo di Software, possono cambiare le modalità di acquisto, di integrazione, sviluppo e aggiornamento. In caso di software commerciali le modalità di implementazione, di testing e di aggiornamento sono indicate dalla società proprietaria, anche tramite System Integrator, fermo restando la verifica da parte di *AULSS n. 9 Scaligera* dell'esistenza delle condizioni minime di sicurezza.

Nel caso in cui *AULSS n. 9 Scaligera* affidi a Società specializzate che utilizzino sistemi Open Source o sviluppino in proprio il software, la società stessa dovrà approntare un piano dettagliato che elenchi le condizioni di sicurezza del software per tutto il ciclo di vita dello stesso.

### 5.1 Authentication, Authorization e Accounting (AAA)

Il Fornitore è tenuto al rispetto delle AAA (Authentication, Authorization e Accounting) su tutti i sistemi che contengano dati di *AULSS n. 9 Scaligera*, personali o di business. Tali regole valgono, oltre per tutti i servizi esposti, anche per applicativi/apparati entro il perimetro di rete di *AULSS n. 9 Scaligera* e per le comunicazioni interne.

#### 5.1.1 Authentication

Il Fornitore deve garantire che l'accesso ai sistemi che contengono i dati oggetto del servizio erogato a *AULSS n. 9 Scaligera* avvenga solo dopo aver superato la fase di "identificazione" e "autenticazione" in modo tale da definire in maniera univoca l'identità dell'utente. *Con l'identificazione il sistema riconosce che l'utente ha un'utenza valida sul sistema.*

*Con l'autenticazione l'utente dimostra di essere il reale possessore dell'utenza fornendo delle credenziali valide.*

Nel caso di applicativi/servizi messi a disposizione per *AULSS n. 9 Scaligera* possono configurarsi due casistiche, in funzione della tipologia di servizio/applicativo, e che dovranno essere concordate preventivamente con *AULSS n. 9 Scaligera*:

- Federazione con il Sistema *AULSS n. 9 Scaligera* di Identity Provider (IdP) - in quel caso le credenziali di accesso sono fornite e mantenute dalla piattaforma di *AULSS n. 9 Scaligera*. Tutte le policy di accesso sono controllate da *AULSS n. 9 Scaligera* (ad esempio tipo di password, scadenza etc). Al Fornitore rimane la logica di identificazione dei profili. In tal caso saranno fornite indicazioni di dettaglio per l'integrazione al sistema di *AULSS n. 9 Scaligera*;
- Gestione degli accessi in locale: in quel caso le credenziali di accesso, le policy e i profili sono contenuti esclusivamente sulla piattaforma. In tal caso il Fornitore deve garantire la piena compliance ai requisiti espressi da *AULSS n. 9 Scaligera*.

La valutazione del tipo di autenticazione da utilizzare, in funzione del tipo di piattaforma informatica, dal tipo di informazione e dalla numerosità degli utenti, sarà concordata con *AULSS n. 9 Scaligera*.

### 5.1.2 Authorization

Indipendentemente dal modello di autenticazione adottato, il sistema deve garantire che gli utenti possano trattare solo il set minimo di dati necessario per eseguire le proprie attività. Le informazioni necessarie sono strettamente legate all'applicativo e alle prestazioni dello stesso. Quindi ogni volta che si desidera accedere ad un dato occorre verificare l'autorizzazione dell'utente. Le restrizioni devono essere garantite attraverso adeguati sistemi di profilazione, che identifichino classi di clienti in funzione del ruolo e della responsabilità.

Il processo autorizzativo per la creazione delle utenze è quello di *AULSS n. 9 Scaligera*. Il Fornitore deve predisporre profili di accesso adeguati a quanto richiesto in fase di definizione del progetto.

### 5.1.3 Accounting

Il sistema deve consentire il tracciamento dell'utilizzo delle risorse da parte degli utenti (Log-in log-out). Devono poter altresì essere tracciabili accessi a dati riservati, sensibili oppure export di dati massivi. Tali log devono essere trasferiti ai sistemi di monitoraggio *AULSS n. 9 Scaligera* secondo modalità che saranno definite in scope alla fornitura, nel rispetto degli ulteriori requisiti forniti di seguito.

### 5.1.4 Requisiti di Autenticazione, Authorization e Accounting

*AULSS n. 9 Scaligera*, richiede che sui sistemi di proprio utilizzo, con particolare rilevanza sui sistemi che contengano dati personali, vengano implementate misure di sicurezza idonee a garantire la confidenzialità dei dati.

Anche a seguito della piena applicazione del GDPR, dove il passaggio dal concetto di requisiti minimi a misure adeguate permette una maggior flessibilità nell'implementazione dei requisiti, prevede che le misure di sicurezza dipendano dalla riservatezza del dato stesso.

Per ogni sistema deve essere effettuata una valutazione e una scelta delle precauzioni di sicurezza e del modo più idoneo di proteggere gli accessi. Tali attività e modalità dovranno essere concordate con il referente del progetto e il dipartimento di Security di *AULSS n. 9 Scaligera*.

Si ribadisce che le password non devono mai essere conservate in chiaro (nei dbms, nei file di configurazione, etc.) ma deve essere adeguatamente protetta tramite password hashing o con metodi di cifratura adeguati. Nessuna password deve essere memorizzata nel codice sorgente di un software. Nel caso di utenze tecniche è possibile la conservazione su file di configurazione in spazi adeguatamente protetti e con accessi limitati, sempre previa verifica di fattibilità con il referente del progetto e il dipartimento di Security di *AULSS n. 9 Scaligera*.

Come best practice, nel caso in cui il software preveda la gestione delle credenziali locali, le password non dovrebbero mai poter essere visualizzate in chiaro da parte del gestore della piattaforma (IT Manager) ma deve essere prevista una modalità di creazione/reset e invio automatico delle password tramite mail/sms/OTP senza ricorrere a modalità insicure di comunicazione delle credenziali e salvaguardare il gestore dal conoscere credenziali assegnate a altri utenti.

Di seguito sono indicati un elenco di requisiti che *AULSS n. 9 Scaligera* richiede per gli accessi. Il Fornitore è tenuto a valutare la compliance del proprio sistema con quanto indicato nell'elenco. Sono considerate valide anche modalità diverse, che possano garantire un adeguato e analogo livello di protezione accertabili anche attraverso test di sicurezza.

Requisiti Authentication <i>si intendono applicabili se il sistema effettua un processo di autenticazione diverso dal sistema di Identity Provider di AULSS n. 9 Scaligera</i>		
01	<p>Gli account di utenti nominali non devono mai essere cancellati e possono trovarsi in due soli stati:</p>	<p><b>attivo:</b> consente l'accesso all'utente che conosce le credenziali per autenticarsi;</p> <p><b>disabilitato / bloccato:</b> non deve consentire l'accesso nemmeno se l'utente conosce le credenziali per autenticarsi. Un account disattivo può ritornare attivo solo se associato all'utente a cui era assegnato precedentemente. Non è possibile assegnare lo stesso account a utenti diversi, nemmeno in tempi diversi. In questo modo vi sarà una corrispondenza univoca tra utente e account. L'azione di riattivazione dell'account deve prevedere uno specifico Log con modalità dicate nel cap. di rif.</p>
02	<p>Il software deve assicurare che la password di un account venga creata e gestita rispettando i seguenti requisiti:</p>	<ol style="list-style-type: none"> <li>1) la password non deve contenere la username, il nome o il cognome dell'utente (non case sensitive);</li> <li>2) la password deve scadere e quindi l'utente deve cambiarla al massimo ogni 3 mesi (deve essere un parametro configurabile su richiesta di <i>AULSS n. 9 Scaligera Security</i>);</li> <li>3) la nuova password non deve essere identica alle 3 precedenti, compresa l'attuale (deve essere un parametro configurabile su richiesta di <i>AULSS n. 9 Scaligera Security</i>);</li> <li>4) la password deve contenere almeno 14 caratteri alfanumerici (deve essere un parametro configurabile su richiesta di <i>AULSS n. 9 Scaligera Security</i>, il valore inferiore deve essere concordato preventivamente). Per software che prevedono l'accesso con l'account di dominio aziendale <i>AULSS n. 9 Scaligera</i>, deve anche essere</li> <li>5) impostato un limite massimo alla lunghezza pari a 30 caratteri per conformità ad alcune limitazioni tecniche degli applicativi <i>AULSS n. 9 Scaligera</i>.</li> <li>6) la password deve soddisfare almeno tre delle seguenti regole:               <ul style="list-style-type: none"> <li>○ deve contenere almeno un carattere maiuscolo;</li> <li>○ deve contenere almeno un carattere minuscolo;</li> <li>○ deve contenere almeno un carattere numerico;</li> <li>○ deve contenere almeno un carattere speciale (es.?\$%&amp;!).</li> </ul>               Per software che prevedono l'accesso con l'account di dominio aziendale <i>AULSS n. 9 Scaligera</i>, i soli caratteri speciali ammessi sono: ?/~!@#\$%^&amp;*()_+ = - ` { } [ ] \ ; : ' &lt; &gt; per conformità ad alcune limitazioni tecniche degli applicativi <i>AULSS n. 9 Scaligera</i>.             </li> <li>7) la password non deve contenere sottostringhe di lunghezza minima 3 caratteri del fullname (unione di nome e cognome), ottenute usando come caratteri delimitatori i seguenti: spazio, trattino ("-"), underscore ("_"), virgola (","), tab. Esempio: la password dell'utente Gian Piero De Rossi non potrà essere "Gian_1970", ma potrà essere "de_reds_1970";</li> <li>8) la password dell'utente deve essere generata dagli utenti amministratori o automaticamente dal software rispettando i punti da 1 a 6 di questo requisito; deve essere resa nota direttamente all'utente attraverso una modalità che impedisca a terzi di appropriarsi indebitamente della password (eventuali modalità diverse dovranno valutare da <i>AULSS n. 9 Scaligera</i>);</li> <li>9) il software, al primo accesso di un utente, deve forzare il cambio password; non deve essere possibile nemmeno per un utente amministratore disabilitare la funzione di cambio password al primo accesso (eventuali modalità diverse dovranno valutare da <i>AULSS n. 9 Scaligera</i>);</li> <li>10) la password deve essere re-inizializzata (dall'utente amministratore o automaticamente dal software) su richiesta</li> </ol>

		<p>dell'utente (es. è stata dimenticata); a seguito di una re-inizializzazione della password il software, al primo accesso, deve forzare il cambio password;</p> <p>11) il software deve bloccare l'account dell'utente nel caso di raggiungimento di 3 tentativi di accesso errati o ritardare successivi tentativi di login (deve essere un parametro configurabile su richiesta di <i>AULSS n. 9 Scaligera Security</i>);</p> <p>12) in caso di blocco dell'account l'utente segnala il problema agli utenti amministratori che provvedono affinché venga generata e resa nota (attraverso il processo descritto al punto 7) una nuova password. A seguito della re-inizializzazione della password il software, al primo accesso, deve forzare il cambio password. Inoltre:</p> <ul style="list-style-type: none"><li>○ gli accessi ai dati di traffico devono essere effettuati in strong Authentication e deve essere consentito solo agli utenti che hanno necessità di accedere a tali dati</li><li>○ gli account devono passare dallo stato attivo allo stato disattivo in modo automatico se l'utente non effettua un accesso al servizio per più di 90 giorni. Se ciò non è possibile, deve essere definito un processo che mensilmente disabiliti gli account che non accedono da più di 90 giorni. Per esigenze specifiche tale termine può essere ridotto ma non può mai eccedere il limite dei 90 giorni.</li><li>○ il servizio deve consentire l'accesso esclusivamente nominale solamente dopo che l'utente è stato correttamente autenticato. Non sono consentiti accessi con account di gruppo o non personali.</li></ul> <p>Non deve essere possibile rinominare l'identificativo univoco dell'account (es. username) se questo è stato già utilizzato almeno una volta.</p>
03	Quando ritenuto necessario, è consentita la presenza di un account non nominale ad uso esclusivo degli utenti amministratori. Tale account può essere utilizzato per accesso diretto all'applicativo solo in caso di emergenza (eventualmente anche bypassando i meccanismi di default predisposti per l'autenticazione degli utenti). Devono essere soddisfatte le seguenti condizioni:	<ul style="list-style-type: none"><li>○ la password deve essere nota solamente agli utenti amministratori;</li><li>○ la password deve essere conservata in modo sicuro (es. in un armadio chiuso a chiave, in un software ad hoc, ...)</li><li>○ le procedure per l'utilizzo dell'account, le modalità di conservazione della password e l'elenco delle persone che compongono il gruppo degli utenti amministratori devono essere documentate e la documentazione deve essere mantenuta aggiornata;</li><li>○ la documentazione deve essere condivisa con la direzione Security di AULSS n. 9 Scaligera in modo che si possano istituire dei punti di controllo;<ul style="list-style-type: none"><li>○ La password di tali utenze tecniche deve poter essere cambiata a cura di personale AULSS n. 9 Scaligera (utenti amministratori AULSS n. 9 Scaligera).</li></ul></li></ul>
04	I flussi dati di tipo host-host devono essere automatici, cioè non deve essere necessario l'intervento manuale di un utente che inserisca le proprie credenziali (salvo in casi eccezionali dovuti ad esempio a malfunzionamenti; in questi casi è necessario tenere traccia delle operazioni manuali eseguite).	
06	I flussi dati di tipo host-host devono utilizzare account dedicati, devono garantire l'autenticazione tra le parti (es. mutua autenticazione con scambio di certificati SSL) e la protezione dei dati scambiati (es. cifratura a livello di trasporto - Layer 4 Modello ISO-OSI). Eventuali password utilizzate per l'autenticazione devono poter essere modificate senza necessità di sviluppi software.	
07	Le interfacce per la fruizione del servizio e/o per la configurazione e manutenzione del servizio esposte su rete pubblica (Internet) devono consentire l'accesso al minor numero possibile di indirizzi IP, che devono essere opportunamente "hardenizzati" in termini di servizi esposti e sanati dalla presenza di vulnerabilità note	
08	A richiesta di AULSS n. 9 Scaligera la soluzione deve prevedere la possibilità di utilizzare un secondo fattore di authentication 2FA o MFA (Multi-Factor Authentication) come: SMS, App Standard come Google, MS e, OATH token)	
Requisiti Authorization		
01	Deve essere prevista una procedura di verifica almeno annuale della necessità di accesso al servizio da parte	

	degli utenti considerando la mansione aziendale di ciascuno (a carico di <i>AULSS n. 9 Scaligera</i> o del Fornitore).	
02	Il profilo assegnato ad un account deve essere scelto da un insieme di profili predefiniti, documentati e già implementati sul servizio. Il profilo scelto per l'account deve consentirgli di eseguire tutte e sole le operazioni che il titolare dell'account ha necessità di effettuare. Deve essere possibile in ogni istante sapere esattamente quali permessi sono associati ad un profilo e quale profilo è associato ad un account. Il software deve impedire di creare un account a cui non è associato un profilo.	
03	Ogni utente può avere una o più mansioni. In ciascuna mansione deve possedere un solo account associato all'adeguato profilo, a meno di specifiche esigenze che dovranno essere formalizzate tra le parti.	
04	Per le sessioni su base utente deve essere sempre configurabile un periodo massimo di validità.	
05	Se possibile effettuare export massivi di dati relativi ad almeno una delle seguenti categorie:	<ul style="list-style-type: none"><li>o clienti</li><li>o prospect</li><li>o dipendenti</li><li>o fornitori/outsourcer</li><li>o partner</li><li>o soggetti terzi rispetto al cliente</li></ul> <p>allora l'applicativo deve consentire la creazione di un profilo che dia la possibilità di assegnare o rimuovere il permesso di eseguire le estrazioni massive.</p>
06	Al fine di poter rispondere alle esigenze normative (soggette a ispezioni da parte delle funzioni interne di controllo e delle Autorità), l'owner applicativo deve fornire a <i>AULSS n. 9 Scaligera</i> ICT Security l'elenco delle operazioni business critical che ritiene siano necessarie al fine di monitorare abusi o azioni illecite (come ad esempio export di dati dal database, etc). E' compito dell'owner applicativo coinvolgere i referenti di <i>AULSS n. 9 Scaligera</i> la validazione delle informazioni business critical da tracciare e a seguire <i>AULSS n. 9 Scaligera</i> ICT Security per fornire i requisiti sul formato e le modalità di trasmissione delle suddette informazioni.	
Requisiti Accounting		
01	Devono essere registrati in tempo reale in log di livello applicativo tutti gli eventi relativi all'export di dati.	
02	Devono essere registrati in tempo reale in log di livello applicativo gli eventi relativi agli accessi (login e logout) eseguiti dagli utenti attraverso le interfacce per la fruizione del servizio e/o per la configurazione e manutenzione del servizio. La registrazione deve avvenire sia per software che utilizzano autenticazione locale, sia per software che utilizzano autenticazione federata.	
03	L'evento di scadenza della sessione di un utente deve essere registrato in tempo reale in log di livello applicativo in modo equivalente ad un evento di logout.	
04	Tutti gli eventi registrati nei log devono sempre contenere almeno le seguenti informazioni:	<p>data e ora in cui si è verificata l'operazione (compreso di fuso orario);</p> <p>i dettagli del software e dell'host che ha generato il log (es. hostname, nome software, modulo, ecc.)</p> <p>l'account che ha eseguito l'operazione e l'identificativo della sua sessione;</p> <p>l'identificativo univoco del dispositivo da cui l'utente ha eseguito l'operazione (es. hostname/IP e porta);</p> <p>l'identificativo dell'evento, i parametri e l'esito;</p> <p>la chiave di correlazione tra eventi, nel caso in cui un'operazione sia tracciata su più righe di log.</p> <ul style="list-style-type: none"><li>o • Deve essere fornita documentazione dettagliata che consenta l'interpretazione degli eventi registrati nel log.</li></ul>
05	Devono essere registrati in tempo reale in log di livello applicativo tutti gli eventi relativi alla visualizzazione e/o alla ricerca massiva sui dati, da interfacce applicative o con accesso diretto al database.	
06	Devono essere registrati in tempo reale in log di livello applicativo tutti gli eventi relativi alla modifica e/o cancellazione dei dati.	
07	Devono essere registrate in log di livello applicativo gli eventi di modifica di un account effettuate dagli user attraverso le interfacce per la fruizione del servizio e/o per la configurazione e manutenzione del servizio.	<p>In particolare, devono essere tracciati almeno i seguenti eventi:</p> <ul style="list-style-type: none"><li>o creazione di una nuova utenza</li><li>o disattivazione di un'utenza esistente (sia disattivazioni manuali sia automatiche)</li><li>o riattivazione di un'utenza disattivata (sia riattivazioni manuali sia automatiche)</li><li>o aggiornamento dell'anagrafica di un'utenza</li><li>o modifica del profilo associato ad un'utenza</li><li>o modifica dei permessi associati ad un profilo</li></ul>



		<ul style="list-style-type: none"> <li>○ reset della password di un'utenza (sia manuale sia automatica)</li> <li>○ • cambio della password di un'utenza</li> </ul>
--	--	--

## 5.2 Posizionamento, retention, cancellazione, portabilità dei dati

I dati di *AULSS n. 9 Scaligera* di norma, indipendentemente che siano dati di business (quindi dati considerati critici come dati finanziari, percentuali di vendita, tassi di guasto di rete) o dati personali, devono risiedere all'interno della Unione Europea. Eventuali necessità di un trasferimento off-shore dei dati dovranno essere preventivamente concordate con il dipartimento di Privacy e di Security di *AULSS n. 9 Scaligera*.

I tempi di retention dei dati di *AULSS n. 9 Scaligera* necessari per compiere le attività contrattualizzate con *AULSS n. 9 Scaligera* devono rispettare i valori concordati con *AULSS n. 9 Scaligera* stessa. Il tempo massimo di archiviazione dei dati trattati dal Fornitore deve essere commisurato in base alla normativa vigente.

Ai sensi del GDPR (Regolamento Privacy Europeo 679/2016) è introdotto il diritto alla cancellazione dei Dati Personali (right to be forgotten) dell'articolo 17.

*AULSS n. 9 Scaligera*, in quanto titolare del trattamento nei casi indicati, è obbligato a procedere alla cancellazione dei dati e per adottare le misure ragionevoli per informare altri titolari del trattamento che stanno trattando i dati, compreso qualsiasi link, copia o riproduzione, per procedere alla cancellazione definitiva dei dati.

Il Fornitore deve quindi garantire adeguate misure e strumenti affinché l'operazione di cancellazione come prevista dalla normativa sia possibile, rapida ed efficace.

La cancellazione permanente dei dati di *AULSS n. 9 Scaligera* o di cui *AULSS n. 9 Scaligera* è Titolare dovrà avvenire, in relazione alla tecnologia di storage adottata, tramite efficaci forme di cancellazione ecc., non conservare traccia in backup o log ecc. In caso di specifica richiesta di *AULSS n. 9 Scaligera*, si dovrà procedere tramite l'utilizzo di appositi strumenti o programmi specializzati (che consentono ad esempio la formattazione a basso livello assicurando la non recuperabilità delle informazioni) al termine del rapporto contrattuale fornendo evidenza scritta mediante autocertificazione ai sensi del DPR 445/2000 che dichiara la cancellazione degli stessi. La cancellazione permanente a basso livello dei dati di proprietà di *AULSS n. 9 Scaligera*, qualora richiesta, dovrà avvenire con tecniche di sanitization fisiche o logiche che rendano impraticabile il recupero dei dati mediante strumenti o procedure di recovery attuate con strumenti commerciali o di laboratorio.

Si faccia riferimento al documento "Guidelines for Media Sanitization", NIST Special Publication 800-88 ([csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)), per avere indicazioni tecniche, in particolare facendo riferimento alle azioni di "purge". L'utilizzo di tecniche anche parzialmente difformi dalle indicazioni del NIST richiede necessariamente il parere del dipartimento di Security di *AULSS n. 9 Scaligera*.

### 5.2.1 Portabilità

In base all'articolo 20 del GDPR, "l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti".

Da quando detto, il Fornitore è tenuto a prevedere nello sviluppo e a condividere con il referente di progetto lato *AULSS n. 9 Scaligera* una soluzione per garantire, se in ambito del servizio, che i dati personali possano essere resi disponibili, in modo semplificato, entro i tempi previsti dal GDPR.

## 5.3 Tracciamento degli accessi e delle operazioni, log e monitoraggio

La normativa sulla registrazione degli accessi (Provvedimento Garante Privacy del 27 novembre 2008) richiede che vengano registrati gli accessi (login) ai sistemi di elaborazione ed agli archivi elettronici effettuati dagli amministratori di sistema. Le registrazioni devono avere "caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità". Le registrazioni debbono comprendere data e ora e la descrizione dell'evento che le ha generate e debbono essere conservate **per almeno 6 mesi**.

Il Fornitore deve essere conforme alle normative vigenti relative a amministratori di sistema, per tutti gli accorgimenti e le misure prescritte per le attribuzioni delle funzioni di amministratore di sistema, volte a prevenire e ad accertare eventuali accessi non consentiti ai dati (personali o di proprietà di *AULSS n. 9 Scaligera*), in specie quelli realizzati con abuso della qualità di amministratore di sistema.

Come da disposizioni di legge, inoltre, è d'obbligo monitorare e **registrare gli accessi effettuati dagli amministratori di sistema ai sistemi contenenti dati personali** (Gazzetta Ufficiale n. 300, 24 Dicembre 2008) anche in linea con gli obblighi di "accountability" sanciti dal Regolamento UE 679/2016 (GDPR). Nello specifico devono essere eseguite le seguenti attività:

- valutazione delle caratteristiche soggettive (due diligence) della capacità e dell'affidabilità del soggetto cui dovranno essere attribuite le funzioni di amministratore di sistema;
- designazione individuale degli amministratori, recante gli ambiti di operatività;
- elenco degli amministratori, contenente gli identificativi e le relative funzioni attribuite ad ognuno;
- verifica periodica delle attività rispetto alle misure di sicurezza previste dalle normative vigenti;
- registrazione degli accessi logici agli archivi elettronici, garantendo completezza, inalterabilità, time stamping e tempi conservazione non inferiori a sei mesi

### 5.3.1 Generazione, conservazione e analisi dei log

In caso di fornitura di un applicativo o di un servizio a *AULSS n. 9 Scaligera*, è necessario che vengano generate, preservate e fornite a *AULSS n. 9 Scaligera* (a richiesta in modo manuale o automatico) alcune tipologie di log di accesso, di tracciamento delle operazioni o di funzionamento dell'applicativo.

I file di log possono rivelarsi molto utili a supporto alla Cybersecurity per la diagnostica e per la fase di Detection.

Dalla loro analisi si possono individuare eventuali malfunzionamenti, anomalie, dati in input che non superano le regole di validazione, intrusioni, azioni illecite e/o non autorizzate da parte degli utenti, modifiche alle configurazioni dell'applicazione, accesso ai dati ai file ed alle risorse dell'applicazione e tipo di accesso, o comunque qualsiasi altro evento rilevante.

Oltre alla registrazione degli accessi, *AULSS n. 9 Scaligera*, in funzione della criticità della soluzione tecnica, raccoglie varie tipologie di log da molti sistemi per effettuare attività di log monitoring, questo per avere un controllo di sicurezza (sia real-time sia ex-post) in merito all'operatività dei sistemi ritenuti critici. In alcuni casi anche le soluzioni informatiche proposte dal Fornitore possono essere nel perimetro di questo controllo e, pertanto, il sistema deve essere adeguato.

In funzione del sistema o della fornitura oggetto di Contratto, il Fornitore dovrà proporre soluzioni idonee in relazione alle tipologie di eventi e log di interesse di *AULSS n. 9 Scaligera*.

I log possono considerarsi di diversi tipi:

- *Log di accesso (obbligatorie)* alla piattaforma detti log-in / log-out (inteso come riusciti e falliti)
  - Il caso in cui il sistema del Fornitore utilizzi la piattaforma di autenticazione di *AULSS n. 9 Scaligera*. In tal caso la piattaforma di *AULSS n. 9 Scaligera* provvederà alla identificazione, creazione e storizzazione dei log di accesso. In questo caso il sistema del Fornitore potrà registrare e conservare i log di accesso alla propria piattaforma per eventuali verifiche, accertamenti o contestazioni;
  - Il caso in cui il sistema di autenticazione del Fornitore sia locale. In tal caso sarà richiesto che tutti gli eventi di autenticazione di log-in, log-out (riusciti e falliti) siano registrati a cura Fornitore e che questi, se necessario in funzione degli accordi presi con *AULSS n. 9 Scaligera*, siano inviati in modo automatico al SOC di *AULSS n. 9 Scaligera*, con tempi e modalità da definire tra le parti.

Per quanto riguarda gli altri tipi di log questi dovranno essere valutati caso per caso con i referenti *AULSS n. 9 Scaligera* e con il dipartimento di Cybersecurity anche in funzione della criticità del servizio e del rischio.

- *Log per il monitoraggio delle operazioni in funzione del tipo di progetto*, ad esempio log di esecuzione delle operazioni massive, log di eventi di copia, log eventi critici, log di azioni che richiedono specifici privilegi, al fine di permettere il controllo su abusi o illeciti. La tipologia e la quantità di log necessaria dovrà essere valutata in funzione delle criticità dei dati e dei relativi trattamenti.
- *Log di sistema*, che servono a tracciare eventi relativi al funzionamento del sistema operativo del server, degli apparati di rete, dei dispositivi di sicurezza.
- *Log generati dai servizi e dai middleware*, che servono a tracciare eventi di funzionamento di software applicativi e analizzare le attività degli utenti applicativi.
- *Log di controllo della soluzione*, ad esempio volti a tracciare le attività svolte da amministratori di sistema o utenti finali e che possono avere un impatto potenziale su integrità, disponibilità e riservatezza dei dati intesi come log specifici della soluzione .

Per quanto riguarda gli altri tipi di log questi dovranno essere valutati caso per caso con i referenti *AULSS n. 9 Scaligera* e con il dipartimento di Cybersecurity anche in funzione della criticità del servizio e del rischio.

Le attività che potranno essere sottoposte a monitoraggio e quindi alla generazione delle registrazioni potranno essere, a titolo di esempio, log di:

- estrazioni massive di dati personali, dati riservati , dati di business, dati economici o bancari;
- eventi di tentata intrusione o violazione regole validazioni;
- visualizzazioni ripetute e reiterate (ad esempio lo scroll/stampa dello schermo);
- eventi di cancellazione, o di copia e/o trasferimento, ad esempio, su supporti esterni;
- accesso ai dati al di fuori dell'orario di lavoro;
- eventi di creazione di utenze o modifica dei privilegi (ad esempio la creazione di utenze admin):
- Accesso alle piattaforme da paesi extra-europei o non in linea con quanto preventivato;

Il Fornitore è tenuto a mettere a disposizione di *AULSS n. 9 Scaligera* tutte le informazioni relative agli utenti che hanno avuto accesso alla piattaforma e, se possibile o se definito in fase di definizione del servizio, i dati consultati e quali operazioni hanno compiuto su tali dati.

Il Fornitore è tenuto (anche in caso di invio continuo/periodico ai sistemi *AULSS n. 9 Scaligera*, salvo indicazione contraria) a conservare obbligatoriamente copia dei log di accesso e delle operazioni definite per un periodo non inferiore a mesi 6, (anche in caso di invio continuo/periodico ai sistemi *AULSS n. 9 Scaligera*, salvo indicazione contraria). Il Fornitore, in ogni caso, è tenuto a fornire la massima cooperazione con *AULSS n. 9 Scaligera* nel caso di giustificati motivi di sospette azioni fraudolente o accidentali, per la risoluzione delle quali serva una analisi approfondita del log.

## 5.4 Requisiti per le interfacce WEB

Le interfacce esposte su Internet, come i portali o le pagine di accesso, presentano un potenziale rischio di attacchi cyber e devono essere adeguatamente protette. Il Fornitore deve garantire che lo scambio di informazioni avvenga con protocolli e modalità che garantiscano l'autenticazione e l'autorizzazione degli accessi, nonché l'integrità e la riservatezza dei dati scambiati.

Le protezioni ai dati devono essere applicate sul sistema sorgente e mantenuta fino al sistema di destinazione (non si deve limitare ai sistemi Edge).

Salvo concordate esigenze tecniche che ne precludano la soluzione, in fase di design del sistema, non si accettano sistemi in cui connessioni HTTPS vengano terminate su bilanciatori o altri nodi intermedi anziché sul frontend dell'applicazione. Anche le connessioni interne devono essere cifrate con meccanismo di mutua autenticazione.

In particolare (ma senza che questi riferimenti costituiscano limitazione o esclusività delle richieste):

- Le interfacce web utilizzate dagli utenti o dagli host, devono basarsi su protocollo HTTPS. Interfacce pubbliche (esposte su Internet) devono avere certificati emessi da una CA pubblica. Interfacce private (esposte solo sulla Intranet) possono avere certificati emessi da CA privata. I servizi accessibili tramite queste interfacce devono essere esposti sulla porta TCP 443. Non possono essere esposte su internet interfacce amministrative di sistema, servizi o middleware.
- Le interfacce web che usano HTTPS (o altri protocolli di comunicazione resi sicuri a livello di trasporto, es. FTPS/SFTP) devono supportare il meccanismo di Perfect Forward Secrecy (PFS). Non si ammettono pertanto versioni di TLS inferiori alla 1.2 e non si ammette l'uso di SSL.

Nel caso in cui l'interfaccia web sia in gestione totale del Fornitore, quindi esterna al perimetro di protezione di *AULSS n. 9 Scaligera*, è richiesta la presenza di un sistema di monitoraggio e di protezione rispetto ad attacchi e tentativi illeciti di accesso. Le interfacce devono essere protette da attacchi quali dagli attacchi DDoS, brute force fino a malware e backdoors.

Tutti i dati strutturati e non strutturati devono essere disponibili per *AULSS n. 9 Scaligera* e forniti su richiesta in un formato standard del settore (es. .doc, .xls, logs e flat files).

## 5.5 Requisiti specifici App Mobile

Nello sviluppo di applicazioni mobili, il Fornitore deve applicare, già a partire dalle prime fasi di progetto, le normative e delle "best practice" internazionali.

Come indicazione non esaustiva, le principali misure devono prevedere:

- l'utilizzo di interfacce utente "user friendly" che indichino quali operazioni di elaborazione dati sono in corso (es. utilizzo di altre app, accesso a funzionalità dell'apparato mobile, accesso alla geolocalizzazione);
- l'utilizzo di identificatori non permanenti (Gli identificatori dei dispositivi devono essere memorizzati esclusivamente per la durata della navigazione)

Una adeguata protezione dei dati con tecniche di hardening sullo storage degli stessi e crittazione dei dati personali;

- l'utilizzo di dati critici e sensibili lato server e non direttamente sull'App o sul dispositivo;
- l'utilizzo di metodi di cancellazione sicura sul dispositivo dei dati;
- che le applicazioni utilizzino protocolli di trasmissione sicura per l'invio di informazioni sensibili attraverso la rete o tramite OTA, quali le credenziali o altri identificativi;
- devono essere implementate misure di sicurezza per prevenire "brute force attack";
- il sistema di gestione delle sessioni deve rispettare le regole standard o definite nell'ambito del progetto per la generazione, la durata e l'utilizzo dei cookie e per le procedure di logout;
- devono essere applicate tecniche di offuscamento del codice per impedire il "reverse code engineering", comprese la codifica di informazioni critiche per il funzionamento dell'applicazione;
- le App e i servizi web per le applicazioni mobili devono essere testati per individuare le vulnerabilità;
- le App devono essere abilitate a rilevare lo stato di rooting/jailbreaking del device;
- le App devono garantire la gestione sicura delle credenziali di accesso tra App e Backend evitando backdoor e credenziali preconfigurate nel codice;
- le App e i servizi web per le applicazioni mobili devono effettuare certificate pinning limitando quali certificati sono considerati validi;
- i sistemi di backend devono essere sottoposti a tecniche di hardening.

Oltre al rispetto delle regole indicate al paragrafo 4.1-Regole per lo sviluppo sicuro del codice, le applicazioni mobile devono essere sviluppate e testate in modo da garantire la conformità anche alle più recenti specifiche OWASP reperibili ai seguenti link :

<https://www.owasp.org>.

<https://owasp.org/www-project-mobile-security/>

<https://owasp.org/www-project-mobile-security-testing-guide/>

<https://owasp.org/www-project-mobile-top-10/>

## 5.6 Requisiti per le interfacce Api

Le API (Application Programming Interface) standard garantiscono in modo semplice l'interoperabilità tra i componenti e per facilitare la migrazione delle applicazioni. Il Fornitore, nel caso renda disponibile questo strumento, è tenuto a fornire dettagli sulle API disponibili indicando:

- Se trattasi di API standard o proprietarie.
- La tecnologia utilizzata e profili di interoperabilità;
- Livello di accesso (Community, Restricted);
- Riferimento al certificato d'accesso utilizzato;
- Aspetti di sicurezza specifici che è necessario conoscere per utilizzare correttamente l'API;
- Aspetti relativi al monitoraggio delle API;
- Gli aspetti relativi al lifecycle delle API e le modalità di aggiornamento

Le API infine devono essere corredate di adeguata documentazione necessaria per l'integrazione nell'ecosistema di AULSS n. 9 Scaligera. Oltre al rispetto delle regole indicate le interfacce API devono essere sviluppate e testate in modo da garantire la conformità anche alle più recenti specifiche OWASP .

## 5.7 Data transfer

Nel caso in cui l'applicativo del Fornitore debba essere integrato o interagisca con un applicativo AULSS n. 9 Scaligera, devono essere rispettate tutte le regole di Sicurezza richieste da AULSS n. 9 Scaligera. La policy di AULSS n. 9 Scaligera prevede che tutte le comunicazioni da e verso terze parti devono essere effettuate in modalità sicura.

Il Fornitore deve garantire che lo scambio di informazioni siano con protocolli e modalità che garantiscano l'autenticazione, l'autorizzazione, l'integrità e la riservatezza dei dati scambiati. Tali protezioni ai dati devono essere applicate sul sistema sorgente e mantenuta fino al sistema di destinazione (non si deve limitare ai sistemi edge).

Per proteggere le trasmissioni si possono utilizzare:

- Sicurezza a livello di trasporto: il protocollo a cui affidarsi è il Transport Layer Security (da TLS 1.2 in su) che, lavorando su reti TCP/IP, consente di utilizzare protocolli sicuri nelle comunicazioni web (HTTPS), email (SMTPS), VoIP, file server, etc;
- Tunneling: tramite VPN M2M fornita da AULSS n. 9 Scaligera, o altre soluzioni da concordare, basate su IPSec
- In taluni specifici casi, sicurezza a livello di protocollo applicativo (da definire mediante specifiche deroghe alle condizioni di cui sopra)

Lo scambio di file in modalità batch deve avvenire attraverso il protocollo SFTP o FTPS. Tale soluzione quindi richiede:

- una comunicazione server-to-server;
- l'utilizzo di IP statici;

- l'autenticazione mediante chiave pubblica

## 5.8 Cifratura dei dati memorizzati

La cifratura descritta è intesa per lo stato "data at rest".

La cifratura dei dati è necessaria quando si conservano dati critici memorizzati in storage locali o di rete e/o dbms e/o in file e/o su supporti di backup, strumenti soggetti a possibili accessi non autorizzati, copie illegale dei file, copie integrali del database, o del furto del server o dei supporti su cui risiedono i dati.

La cifratura deve essere efficace in modo tale che, anche se i dati siano sottratti in modo illegittimo, nessuno li possa utilizzare. La cifratura è qui intesa per lo stato "data at rest". Il Fornitore deve garantire la riservatezza delle informazioni attraverso l'utilizzo di protocolli di crittografia dei dati, in modo tale da garantire la riservatezza e l'integrità delle informazioni. Inoltre, i dati devono essere cifrati anche a bordo degli eventuali sistemi di elaborazione utilizzati dalla società e nelle copie (es. backup), salvo l'adozione di sistemi di backup strutturati e centralizzati di rete, per i quali possono valere accorgimenti specifici da validare in sede progettuale.

Le strategie seguite sono tre:

- cifratura a livello applicazione
- cifratura a livello del file system
- cifratura a livello del database

In caso di cifratura parziale, ad esempio cifratura parziale a livello applicativo dei soli dati critici, o di impossibilità tecniche per una cifratura E2E, deve essere effettuata una analisi della criticità in accordo con la funzione Security di AULSS n. 9 Scaligera. Sono considerati dati critici i dati di Business Riservati e i Dati Personali di cui AULSS n. 9 Scaligera è Titolare o Responsabile.

Quando è necessario memorizzare una password, questa non deve essere conservata in chiaro (nei dbms, nei file di configurazione, etc.) ma deve essere adeguatamente protetta tramite password hashing o con metodi di cifratura adeguati. Nessuna password deve essere memorizzata nel codice sorgente di un software. Nel caso di utenze tecniche è possibile la conservazione su file di configurazione in spazi adeguatamente protetti e con accessi limitati, sempre previa verifica di fattibilità con il Owner di Progetto di AULSS n. 9 Scaligera.

## 5.9 Affidabilità e Backup

Viene posta particolare attenzione all'affidabilità e sicurezza dell'infrastruttura con logiche di protezione e riservatezza dei dati e architetture di antispying, antivirus, patching e backup oltre a protezione compatibile SSL/TLS anche senza far ricorso a VPN.

Deve essere valutato con il Contract Manager di AULSS n. 9 Scaligera:

1. Il livello di affidabilità del sistema (inteso come valutazione di disponibilità del servizio);
2. Modalità di Backup di applicativi e dati;
3. Procedure di DR e attività di ripristino (se non già definite dalla BC di AULSS n. 9 Scaligera)

Devono essere definite le misure minime a garanzia di un possibile e rapido ripristino del sistema/applicativo in caso di fault generale danno alle infrastrutture o causato da attacchi di tipo cyber. Devono essere quindi documentate dettagliatamente le modalità operative per un efficace ripristino.

Il Fornitore è tenuto a mettere in atto tutte le protezioni adeguate a preservare i servizi e dati di AULSS n. 9 Scaligera tra cui,

ad esempio:

- devono risultare regolarmente e sistematicamente effettuati i backup off-site; i supporti utilizzati devono risultare cifrati e trasportati in sicurezza.
- devono risultare impiegate tecniche per il monitoraggio della capacity dei sistemi che supportano l'erogazione dei servizi del Fornitore.

Per quanto riguarda il backup delle applicazioni e dei dati contenuti, per poter effettuare procedure di Disaster Recovery, si tenga presente che è necessario:

- Effettuare con regolarità, in funzione del tipo di applicativo e funzione della criticità del sistema, una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
- Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.
- Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.
- Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.

- Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente anche di effettuare la remotizzazione del backup anche in storage remoti, come ad esempio, Cloud o dischi remoti.
- Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

Per l'attività di ripristino, devono essere disponibili e consegnati alla struttura operativa che si occupa dell'esercizio in produzione dell'applicativo la documentazione e le procedure per l'attività di ripristino.

## 6 Sicurezza della componente Hardware e delle infrastrutture, Cloud

Il Fornitore per la fornitura di software/applicativi/dispositivi, può concordare con AULSS n. 9 Scaligera, il posizionamento della piattaforma fisica degli applicativi.

Le soluzioni sono essenzialmente:

- Soluzioni on-premises – Come dice il termine stesso, sono soluzioni installate sui computer di ogni singolo utente o su un server aziendale;
- Soluzioni Cloud – Questo tipo di soluzioni sono servizi offerti da un provider, accessibili via internet attraverso una piattaforma virtuale e tipicamente ospitata e gestita da un fornitore di terze parti.

Nel caso in cui le soluzioni on-premises o Cloud siano fornite da AULSS n. 9 Scaligera, la sicurezza fisica e infrastrutturale è garantita da AULSS n. 9 Scaligera stessa.

Nel caso in cui il Fornitore utilizzi piattaforme proprie oppure si avvalga di spazi o cloud di terzi, dovrà verificare e garantirne la sicurezza.

Di seguito sono indicati requisiti specifici per diverse casistiche.

### 6.1 Applicativi posizionati nei data center presso il Fornitore

Nel caso in cui il servizio presso proprie sedi/spazi comprenda l'esercizio di sale dati proprietarie, il Fornitore deve garantire, oltre a quanto indicato nel paragrafo relativo alla protezione di sicurezza fisica anche quanto riportato di seguito.

Il personale che fornisce o si occupa dei servizi di manutenzione agli impianti di supporto deve accedere alle aree protette solamente quando ciò effettivamente necessario e solo dietro autorizzazione del Responsabile delle infrastrutture. Ove necessario, l'accesso deve essere limitato controllando le attività del personale esterno.

Devono valere almeno le seguenti condizioni di sicurezza per i locali che ospitano i sistemi inerenti al servizio:

- a) ai visitatori ed ai dipendenti non autorizzati permanentemente all'accesso alla sala dati deve essere concesso l'accesso solamente per scopi specifici ed autorizzati dal Responsabile delle infrastrutture. Tali accessi devono essere registrati in un apposito documento/registro;
- b) devono essere installati adeguati sistemi di emergenza, rispondenti alle normative statali e locali, quali rivelatori di fumo, sensori della temperatura, sensori antiallagamento, allarmi antincendio, estintori e vie di fuga in caso di incendi. Il sistema di emergenza deve essere in grado di riportare le segnalazioni di allarme a postazioni di controllo e gestione centralizzate e remote. I sistemi e le relative procedure di emergenza devono essere controllati e rivisti ad intervalli regolari seguendo le istruzioni del fabbricante. I dipendenti devono ricevere un'adeguata istruzione all'utilizzo dei sistemi di emergenza;
- c) deve essere assicurata l'alimentazione in caso di black-out da gruppi di continuità (UPS) di adeguata potenza e capacità in modo da sostenere un carico normale per il tempo necessario all'avvio del gruppo elettrogeno;
- d) la protezione fisica delle sale dati deve essere dimensionata per prevenire le effrazioni e gli incidenti. In tale senso dovrà essere costituita un'adeguata area di protezione perimetrale non di facile scavalco, manomissione o penetrazione (per esempio grigliati metallici o pareti in muratura) e dovrà essere posta particolare attenzione qualora l'area sia posta in prossimità di sedi stradali o comunque di movimentazione mezzi meccanici per prevenire l'abbattimento accidentale della stessa.

Deve essere garantito il pronto intervento delle forze dell'ordine o di una società di vigilanza privata.

### 6.2 Applicativi posizionati al di fuori del perimetro fisico di AULSS n. 9 Scaligera/Fornitore

AULSS n. 9 Scaligera, alla luce della specifica natura delle proprie attività, richiede lo sviluppo e/o la fornitura di dispositivi destinati ad essere ospitati al di fuori dai Data Center dell'azienda o comunque dal perimetro di sicurezza stabilito dal Fornitore. Si tratta di dispositivi quali (a titolo esemplificativo) CPE, antenne o altri oggetti che, pur posizionati in contesti fisici che non garantiscono elevati standard di sicurezza (es. nelle abitazioni di clientela consumer, in cabinet/installazioni esterni, ecc.) sono tuttavia connessi con reti e sistemi AULSS n. 9 Scaligera.

Tali sistemi sono tipicamente dotati di interfacce fisiche di connessione e possono essere gestiti remotamente o attraverso la connessione a porte locali. Queste tipologie di accessi, se non adeguatamente messi in sicurezza, possono dare luogo a violazioni che dal device stesso possono estendersi ai sistemi interni di AULSS n. 9 Scaligera (anche in relazione ai c.d. "supply chain attacks"). L'accesso alle parti interne del dispositivo stesso, se non adeguatamente protetto, può portare a tale risultato, esponendo all'azione di un eventuale attaccante componenti, connessioni e/o interfacce fisiche non accessibili esternamente.



Tali sistemi inoltre sono tipicamente dotati di meccanismi e funzionalità per l'aggiornamento del software/firmware, anche in relazione alle necessità di correzione di vulnerabilità di sicurezza che dovessero emergere nel corso del ciclo di vita dell'oggetto stesso (oltre che di evoluzione delle funzionalità). Nel caso specifico in cui i sistemi siano posizionati all'esterno del perimetro fisico di sicurezza, è obbligatorio che tali aggiornamenti debbano avvenire in modalità sicura attraverso meccanismi che consentano di prevenire l'installazione di firmware manipolato che possa alterare il comportamento degli oggetti abilitando gli attacchi di cui sopra. Al fine di minimizzare la possibilità di tali eventi, in relazione alla tipologia di oggetto in perimetro alla Fornitura, AULSS n. 9 Scaligera potrà richiedere al Fornitore, in relazione alla natura del dispositivo stesso, accorgimenti quali:

- ❖ Accorgimenti atti ad innalzare la sicurezza delle interfacce e delle porte fisiche:
  - tutte le interfacce di programmazione e/o debugging devono risultare disattivate a livello hardware sui prodotti in produzione, ad esempio rimuovendo o disabilitando permanentemente tutte le porte di programmazione presenti sulle schede elettroniche (con particolare attenzione alle porte JTAG).
  - Alternativamente alla disabilitazione hardware è consentita la disattivazione permanente via software (ad esempio mediante adozione di accorgimenti quali Secure Jtag 1 o similari in relazione alla tipologia di oggetto).
- ❖ Meccanismi antintrusione e a contrasto del "reverse engineering":
  - In relazione alla natura stessa del dispositivo, con particolare riferimento all'eventuale installazione in ambienti esterni e/o non presidiati, il dispositivo dovrà essere dotato di soluzioni di protezione all'accesso alle componenti interne che siano "tamper resistant", prevenendo almeno che tutte le viti esterne allo chassis siano di tipo non standard (security torx with pin, tri-wing, ecc.).
  - Sempre in relazione alla natura stessa del dispositivo, si potrà richiedere che esso sia dotato di soluzioni di "tamper detection", in particolare mediante la presenza di switch in grado di rilevare l'apertura dello chassis dell'oggetto. Il cambio di stato dello switch dovrebbe inoltre poter eseguire un comando arbitrario sul sistema (ad esempio effettuare lo spegnimento del sistema, il lancio di uno script, l'attivazione di un "kill-switch" di varia natura, l'invio di un evento syslog a sistemi di raccolta, ecc.), e tale comportamento dovrebbe essere configurabile secondo le indicazioni fornite da AULSS n. 9 Scaligera.
  - AULSS n. 9 Scaligera potrà richiedere che il rilevamento del cambio di stato dello switch possa avvenire anche a dispositivo non alimentato (ad es. mediante registri di memoria e batteria tampone) così da massimizzare la probabilità che l'evento possa essere acquisito/gestito al successivo riavvio.
  - In generale, si richiede l'adozione di misure di "tamper evidence", che potranno andare dall'apposizione di appositi "sigilli" atti a rendere evidente l'apertura del dispositivo, sino ad accorgimenti più complessi da definirsi.
- ❖ Meccanismi a supporto dell'integrità del firmware e dell'avvio del dispositivo:
  - Il Fornitore deve provvedere alla disabilitazione delle funzionalità di Boot interattivo eventualmente offerte dal Bootloader inibendo completamente la possibilità di modificare le configurazioni del Bootloader e rendendo impossibile effettuare il boot storage/periferiche esterne. Ove possibile, si richiede l'adozione di funzionalità di "secure boot" o similari.
  - In aggiunta e a complemento delle misure presenti nelle politiche e linee guida AULSS n. 9 Scaligera inerenti le modalità di accesso sicuro ai sistemi e la minimizzazione dei servizi esposti, a supporto della - possibilità di effettuare in modo sicuro l'aggiornamento del firmware del dispositivo si richiedono funzionalità quali: firma digitale o altri meccanismi di controllo dell'integrità degli aggiornamenti rilasciati; possibilità di effettuare lato device la verifica di integrità abilitata dal punto precedente prima dell'installazione dell'aggiornamento; supporto a meccanismi di aggiornamento standard resi disponibili dalla tipologia di sistema operativo/embedded OS montato sul device.

## 6.3 Norme per l'utilizzo del Cloud

Nel caso in cui i software/applicativi siano installati su piattaforme Cloud pubbliche si possono individuare 3 casistiche:

- 1) Cloud di AULSS n. 9 Scaligera. In questo caso AULSS n. 9 Scaligera è responsabile della piattaforma e quindi il Fornitore deve rispettare le regole per l'utilizzo del Cloud indicate da AULSS n. 9 Scaligera all'atto del contratto di fornitura del Cloud
- 2) Cloud Azure/AWS: Le piattaforme Microsoft/Amazon sono tra le più conosciute. Essendo state utilizzate più volte da AULSS n. 9 Scaligera sono considerate come certificate in modo analogo al Cloud di AULSS n. 9 Scaligera. L'unica attenzione aggiuntiva è che il posizionamento dei dati deve essere all'interno dell'Unione Europea, fatto salvo deroghe o eccezioni da concordare.
- 3) Cloud di terzi: In questo caso il Fornitore è tenuto a presentare tutta la documentazione di sicurezza del provider Cloud (dalla documentazione tecnica ai test di sicurezza) e AULSS n. 9 Scaligera si riserva di verificare la



validità della soluzione e della protezione alla cyber-security , in funzione anche dei dati trattati e della criticità dell'applicativo software.

Di seguito le certificazioni richieste, i requisiti e le linee guida generali per l'adozione e utilizzo del cloud computing nell'erogazione di servizi per AULSS n. 9 Scaligera:

- a) Per garantire un elevato livello di sicurezza e standard di qualità, i servizi forniti dalla soluzione proposta devono essere certificati ISO 9001, ~~14001, 20000~~ e 27001;
- b) Se la soluzione proposta offre alcuni o tutti i servizi che utilizzano infrastrutture cloud, tali servizi devono essere certificati CSA STAR. Il Fornitore della soluzione, quindi, è tenuto a fornire link al registro CSA STAR Registry dove vengono pubblicate le prove di autovalutazione e/o di certificazione STAR;
- c) Se la soluzione prevede l'utilizzo di una piattaforma di Cloud di terzi come, ad esempio, Azure o AWS, il Fornitore è tenuto a indicare e aggiornare con continuità AULSS n. 9 Scaligera del tipo di piattaforma utilizzato per la soluzione e ogni eventuale variazione;
- d) In caso di servizio IaaS tutti gli aggiornamenti riguardanti la piattaforma utilizzata sono a cura del fornitore garantendo la compatibilità delle applicazioni e del servizio per AULSS n. 9 Scaligera;
- e) Il Fornitore della soluzione deve dichiarare esplicitamente dove conserva fisicamente i dati trattati ed elaborati. Se il luogo fisico dove sono posizionati i dati (data center o cloud) non è situato esclusivamente In Italia o in UE, Il Fornitore è tenuto a informare AULSS n. 9 Scaligera per predisporre l'adeguata documentazione autorizzativa;
- f) Il Fornitore, nell'utilizzo del Cloud, deve costantemente monitorare che sia garantita la disponibilità, la qualità, la capacità adeguata delle risorse, le prestazioni del servizio. Le proiezioni dei futuri requisiti di capacità devono essere effettuate per ridurre il rischio di sovraccarico del sistema;
- g) Il Fornitore anche per il servizio Cloud deve verificare che le proprie applicazioni siano immuni dalle più comuni vulnerabilità (come già precedentemente specificato) e risolvere eventuali criticità prima dell'implementazione nell'ambiente di produzione.
- h) L'utilizzo di accessi alle interfacce amministratore tramite autenticazione a 2 fattori (2FA o MFA Multi-Factor Authentication) e relativi log di accesso eventualmente da inviare a AULSS n. 9 Scaligera come indicato nel cap. 5.2.
- i) Tutte le infrastrutture (immagini guest) utilizzate devono essere sottoposte periodicamente ad attività di hardening.

## 6.4 Sicurezza di infrastrutture basate su virtualizzazione e/o container

Nel caso in cui una soluzione basata su Virtualizzazione/Container sia posizionata su Datacenter di AULSS n. 9 Scaligera, tutte le regole di sicurezza fisica sono demandate alle policy interne di AULSS n. 9 Scaligera. Nel caso in cui si utilizzino Datacenter del Fornitore o di terzi, le regole sono indicate ai paragrafi 6.1 e 6.2.

Tutte le infrastrutture devono essere sottoposte periodicamente ad attività di hardening dei sistemi operativi

### 6.4.1 Virtualizzazione

Dal punto di vista della sicurezza le seguenti sono raccomandazioni di sicurezza sono consigliate per l'hypervisor:

- Installare tutti gli aggiornamenti dell'hypervisor appena disponibili;
- Limitare l'accesso amministrativo alle interfacce di gestione dell'hypervisor usando una rete di gestione dedicata o la gestione le comunicazioni di rete autenticate e crittografate utilizzando moduli crittografici convalidati FIPS 140-2.
- Sincronizzare l'infrastruttura virtualizzata con un server orario sicuro;
- Scollegare l'hardware fisico inutilizzato dal sistema host;
- Disabilitare tutti i servizi dell'hypervisor come la condivisione di appunti o file tra il sistema operativo guest e l'host OS se non strettamente necessari;
- Monitoraggio della sicurezza e delle attività che avvengono tra i sistemi operativi guest
- monitoraggio continuo dell'auto-integrità che gli hypervisor possono fornire e il monitoraggio e l'analisi dei log.

### 6.4.2 Container

Un container si può considerare come un server virtualizzato ma solo per lo spazio utente, ossia la parte virtualizzata è l'ambiente di esecuzione delle applicazioni e non tutti i componenti sottostanti. Il sistema operativo e il kernel dello stesso sono in comune a tutti i container avviati sulla macchina host. In questo modo non esiste hypervisor, ma è presente solo un sistema che impacchetta le applicazioni o i servizi applicativi in container, gestendone l'attivazione e la disattivazione dei container stessi e creando un livello di astrazione fra questi e il sistema operativo che li ospita.

Dal punto di vista della sicurezza i container dipendono sostanzialmente dalle risorse del sistema host sottostante. Dovrà quindi essere buona regola:

- Assicurarsi che i processi nei container non vengano eseguiti come root.
- I file system andrebbero eseguiti in sola lettura in modo da evitare che un attaccante possa andare a sovrascrivere i dati o salvare degli script dannosi.
- Limitare le chiamate di sistema che un'applicazione può effettuare al kernel, al fine di ridurre la superficie di attacco.
- Limitare le risorse che un container può utilizzare, per evitare che un'applicazione se compromessa possa consumare un elevato numero di risorse tale da portare l'intero sistema in blocco a causa di un Denial Of Service (DoS).
- Limitare riavvio dei container, dell'accesso ai file system, delle Capabilities che possono essere assegnati ai processi per fornire loro un maggiore accesso al sistema
- Prevedere regolari attività di auditing.

## 7 Sviluppo Sicuro aggiornamenti e life cycle

### 7.1 Regole per lo sviluppo sicuro del codice

AULSS n. 9 Scaligera ha definito i requisiti di sicurezza che devono necessariamente essere implementati all'interno di tutti gli applicativi sviluppati in-house, in outsourcing o gestiti da AULSS n. 9 Scaligera.

I requisiti si applicano a tutti gli applicativi sviluppati a prescindere dal processo di sviluppo software (SLDC) adottato come ad esempio agile, waterfall.

Lo sviluppo di codice sicuro consiste negli accorgimenti tecnici da adottare durante la realizzazione delle applicazioni informatiche al fine di prevenire l'introduzione di vulnerabilità che possono essere sfruttate per minacciare la sicurezza del patrimonio informativo di AULSS n. 9 Scaligera.

Agli sviluppatori è richiesto di adottare le best practice di riferimento per la stesura del codice nel linguaggio di programmazione utilizzato sulla specifica architettura di riferimento (Ad esempio, per le applicazioni web, OWASP Development Guide reperibile al seguente link:

[https://www.owasp.org/index.php/OWASP\\_Guide\\_Project](https://www.owasp.org/index.php/OWASP_Guide_Project)

I principi generali di sviluppo sicuro prevedono che:

- le attività di sviluppo devono essere svolte in un ambiente dedicato, diverso da quello di produzione e il codice sorgente deve essere modificato e compilato da parte del solo personale autorizzato;
- durante lo sviluppo, il codice deve essere scritto in modo facilmente comprensibile, corredato da commenti che spieghino il ruolo delle funzionalità ma non siano in numero eccessivo o invasivo, privilegiando in tal senso la chiarezza dei nomi di variabili e funzioni, e ben documentato;
- deve essere garantita l'integrità e la tracciabilità di tutte le modifiche effettuate durante lo sviluppo dell'applicazione tramite strumenti per il versioning, usando le medesime soluzioni per mantenere allineata la relativa documentazione prodotta;
- non devono essere utilizzati codici già sviluppati (API, moduli, macro, librerie, etc.) che siano affetti da vulnerabilità note o che siano ritenuti non sicuri.
- al termine dello sviluppo di ciascuna "unità", essa sia sottoposta almeno a scansioni statiche per la verifica del rispetto delle regole di programmazione sicura.
- al termine dell'integrazione di unità in porzioni di software eseguibili, anche se incomplete, quanto prima si sottoponga il semilavorato a strumenti per la scansione dinamica finalizzata alla ricerca di anomalie di sicurezza nel comportamento.
- Un VA/PT finale come indicato nel par. dedicato presente successivamente.

I requisiti di sicurezza definiscono come l'applicazione dovrà lavorare dal punto di vista della sicurezza. I requisiti di sicurezza devono garantire la conformità con le normative esterne e interne di riferimento in ambito di sicurezza delle informazioni (es. Privacy, PCI-DSS, policy aziendali etc.). I temi della sicurezza riguardano:

- Authentication, Authorization e Accounting
- Gestione delle utenze e utenze tecniche
- Gestione delle sessioni e degli ambienti di sviluppo e produzione
- Sanificazione e verifica dei dati in Input/Output
- Sicurezza nello scambio dei dati
- Code Review
- Uso di software Commerciali

Inoltre, è indicato che l'attività di code review (analisi statica del codice) sia integrata tramite l'utilizzo di strumenti automatizzati al fine di identificare a monte le vulnerabilità del codice realizzato e attività di Penetration Test prima del rilascio in produzione del software sviluppato. L'analisi automatizzata e manuale deve essere svolta considerando tutte le principali problematiche e vulnerabilità note di sicurezza (ad esempio SQL Injection, XSS, CSRF, DOS, etc.), eventualmente personalizzando la lista dei controlli previsti dagli strumenti automatizzati.

### 7.2 Aggiornamento del prodotto software e delle piattaforme

La security posture di un sistema muta nel tempo in relazione all'evoluzione del sistema stesso, ma anche all'eventuale scoperta di vulnerabilità nello stack software (o firmware, in relazione alla tipologia di sistema) utilizzato per la realizzazione delle funzionalità, con riferimento esemplificativo a: sistema operativo, middleware, librerie, demoni/servizi di sistema derivanti da personalizzazioni, software di base/applicativo, ecc.

Con modalità da dettagliarsi in relazione alla specifica Fornitura, e per l'adozione delle quali il Fornitore è tenuto a cooperare con AULSS n. 9 Scaligera in modo proattivo suggerendo le più opportune modalità di attuazione, si richiede l'adozione dei seguenti accorgimenti qui espressi in forma sintetica:

- i sistemi operativi, software, middleware etc. devono essere selezionati nell'ambito di versioni mantenute e non "end-of-life" / "end-of-support", al momento della fornitura e possibilmente per un

congruo periodo di tempo successivo in relazione alla vita utile del sistema. Sono parimenti da evitare (nell'ambito dei componenti software identificati) configurazioni, invocazioni, setting, modalità di utilizzo o quant'altro si abbia evidenza possa essere deprecato e non supportato al momento dello sviluppo/integrazione o nel prevedibile futuro;

- i sistemi operativi, software, middleware etc. devono essere supportati (da vendor/community) in termini di rilascio/disponibilità di aggiornamenti, patch, fix per gli aspetti di sicurezza;
- dovrà in ogni caso essere sempre possibile effettuare l'aggiornamento di security patch/fix, pertanto evitando qualsiasi sviluppo e integrazione che non sopravviva a tale operazione;
- il Fornitore dovrà evidenziare tempestivamente, e quanto prima possibile in sede di progettazione del servizio, l'eventuale vincolo rispetto all'adozione di versioni major di sistemi operativi, software, middleware ecc. che costituiscano limite superiore all'ulteriore evoluzione delle stesse. AULSS n. 9 Scaligera desidera infatti promuovere la realizzazione di sviluppi/integrazioni potenzialmente resilienti all'aggiornamento delle componenti software che li sostengono (con particolare riferimento alla possibilità di mantenere nel tempo la security posture stabilita per il sistema), pertanto saranno da evitare (o comunque da autorizzare espressamente lato AULSS n. 9 Scaligera) sviluppi/integrazioni che non consentano ulteriori upgrade delle componenti software sottostanti;
- sono da evitare (o comunque da autorizzare espressamente dal dipartimento di Security di AULSS n. 9 Scaligera) modifiche, personalizzazioni o customizzazioni a specifiche versioni dello stack software che sostiene l'erogazione delle funzionalità del sistema/servizio, se non riproducibili in modo automatico nelle successive evoluzioni dello stack per un orizzonte temporale presumibilmente congruo rispetto alla vita utile del sistema/servizio stesso. Tali modifiche sono ammesse solo in via transitoria e avendo previamente identificato la soluzione definitiva che consenta la riconduzione ad uno stack aggiornabile in conformità con i rilasci dei vendor e/o della community che sostiene i vari elementi.

### 7.3 Gestione degli aggiornamenti del Software

Si ribadisce al fornitore che la necessità del software di essere costantemente aggiornato è parte integrante della fornitura, pertanto è richiesta garanzia che il software/firmware fornito sia esente da vulnerabilità nel tempo, tramite aggiornamenti o patch, e deve dare un periodo di garanzia per:

- un periodo minimo due anni
- periodi superiori anche a due anni se definiti contrattualmente o se definiti estensioni come contratti di manutenzione o evolutivi pluriennali)

Durante il periodo di garanzia il Fornitore è tenuto a sanare tutte le vulnerabilità presenti a proprie spese.

AULSS n. 9 Scaligera ha in essere un insieme di processi/procedure per le attività di release management/patch management per l'aggiornamento del software in ambiente di produzione.

Sotto il nome di Gestione degli aggiornamenti del Software che consta di:

- Verifica di disponibilità del software/aggiornamenti/Patch/Patch di sicurezza
- Reperimento delle versioni/patch di aggiornamento
- Valutazione dell'impatto
- Fase di testing
- Implementazione
- Collaudo e controllo delle funzionalità del software.

Tale processo permette di distribuire in modo efficiente le applicazioni e gli aggiornamenti garantendo al tempo stesso l'integrità e la sicurezza dell'ambiente di produzione.

Al Fornitore è richiesto di adeguare il proprio processo per la soluzione offerta affinché sia idoneo, ovvero:

- rendere disponibile a AULSS n. 9 Scaligera e adeguatamente documentati gli aggiornamenti necessari affinché AULSS n. 9 Scaligera avvii con successo l'aggiornamento;
- provvedere a fornire aggiornamenti durante il periodo di garanzia e/o per tutta la durata del contratto di manutenzione dando visibilità a AULSS n. 9 Scaligera delle attività in corso e fornendo gli esiti dei collaudi effettuati;

La documentazione prodotta sarà conservata nella cartella di progetto a cura del owner del Progetto di AULSS n. 9 Scaligera.

### 7.3.1 Portale o strumenti del Fornitore per gli aggiornamenti

Nel caso in cui il Fornitore hardware/software metta a disposizione gli aggiornamenti per l'installazione a cura AULSS n. 9 Scaligera, siano essi richiesti da AULSS n. 9 Scaligera sia o generalizzati per miglioramenti o per mitigare eventuali vulnerabilità, è tenuto a garantire una modalità di trasferimento del software modalità sicura e certificata.

AULSS n. 9 Scaligera richiede quindi che il Fornitore, se applicabili :

- a) Disponga di un sito/repository dove siano pubblicati gli aggiornamenti e la documentazione a corredo dove è possibile prelevare e trasferire i file in modo sicuro. In alternativa, se non presente, il Fornitore potrà depositare il software e la documentazione su uno spazio ( su un repository sicuro da definire tra le parti o concordare altro meccanismo di invio che permetta a AULSS n. 9 Scaligera di verificare inoppugnabilmente l'autenticità della sorgente (es. via email firmate/cifrate PGP previo scambio chiavi pubbliche). Il trasferimento del software di persona dovrebbe essere applicabile solo nella fase di prima installazione e deve essere concordata ogni volta con il manager AULSS n. 9 Scaligera di riferimento.
- b) Implementi o disponga di un sistema di avviso, tramite mail, della presenza di aggiornamenti, per informare AULSS n. 9 Scaligera della disponibilità;
- c) Effettui una Pre-valutazione della patch evidenziando gli impatti sui servizi di AULSS n. 9 Scaligera e con particolare evidenza delle risoluzioni a bug-fixing, patch di sicurezza e di disponibilità del sistema
- d) Disponga di un metodo di validazione del software/e firmware attraverso attività di verifica sull'integrità del prodotto (firma, hash etc). Questo metodo deve essere in grado di permettere a AULSS n. 9 Scaligera di eseguire autonomamente la convalida sul software acquisito.
- e) Garantisca l'integrità e la confidenzialità nel trasferimento del software e delle firme;

Eventuali modalità diverse, anche in fase transitoria, devono poter garantire il medesimo livello di sicurezza e dovranno essere concordate con il referente della cybersecurity di AULSS n. 9 Scaligera.

## 8 Verifiche di sicurezza su applicativi e sistemi

Nel caso di fornitura di software/applicativi/sistemi per AULSS n. 9 Scaligera, il Fornitore è tenuto a esibire la idonea documentazione con la quale evidenzi il rispetto delle misure di sicurezza e una certificazione di aver condotto in autonomia verifiche di sicurezza quali Vulnerability Assessment (VA) o Penetration Test (PT). Tale documentazione può essere rappresentata dagli esiti di tali attività (o di opportuni estratti che a giudizio di AULSS n. 9 Scaligera permettano la comprensione delle attività di verifica e remediation svolta) o da certificazioni di mercato, emesse da enti terzi, che tra i punti considerati includano anche la corretta attuazione di tali processi, dalla verifica periodica all'applicazione delle remediation.

AULSS n. 9 Scaligera in ogni caso si riserva la possibilità di effettuare ulteriori verifiche di sicurezza VA o PT, anche tramite terzi, concordando preventivamente il Fornitore le modalità e il perimetro dei test.

Nel caso di verifiche su apparati fisici (CPE, PE, ecc.), il Fornitore è tenuto a mettere a disposizione di AULSS n. 9 Scaligera un congruo (ragionevolmente minimo) numero di apparati atti all'effettuazione di test fisici potenzialmente distruttivi per l'apparato stesso ai fini di testarne la resistenza a tentativi di compromissione e accesso alle componenti interne nonché del processo di aggiornamento firmware.

### 8.1 Documentazione, verifiche e certificazioni di sicurezza del Fornitore

**Il Fornitore dovrà produrre documentazione tecnica di sicurezza in fase di progettazione e durante l'intero ciclo di vita dello sviluppo e renderla disponibile a AULSS n. 9 Scaligera, per eventuali valutazioni di sicurezza.**

Il Fornitore deve sviluppare, documentare e implementare procedure per il rilevamento di eventuali vulnerabilità nella sicurezza, incluso il rilevamento delle vulnerabilità della sicurezza della struttura informatica. Le procedure dovranno contenere la soluzione per il contenimento e la risoluzione delle vulnerabilità.

Sulla base di valutazioni periodiche di opportunità, il Fornitore dovrà quindi condurre analisi di vulnerabilità e penetration test su tutte le applicazioni e infrastrutture che contengono dati riconducibili a AULSS n. 9 Scaligera almeno con frequenza annuale.

Su richiesta di AULSS n. 9 Scaligera, il Fornitore sarà tenuto a fornire gli esiti di tali analisi al Titolare.

### 8.2 AULSS n. 9 Scaligera Security Assessment (VA/PT)

Per valutare i rischi di tipo informatico, AULSS n. 9 Scaligera si riserva di effettuare ulteriori verifiche specifiche al fine di prevenire la messa in produzione di sistemi vulnerabili.

Su richiesta di AULSS n. 9 Scaligera potrà essere effettuato un approfondito Security Assessment (Vulnerability Assessment e Penetration Test) direttamente da personale AULSS n. 9 Scaligera o tramite la collaborazione di aziende di settore specializzate, possibilmente prima della messa in produzione della fornitura informatica. Il Fornitore dovrà collaborare e prestare la massima assistenza per eseguire in modo corretto e efficace il test. Eventuali attività di predisposizione degli ambienti di test e il supporto all'esecuzione dei test saranno senza oneri per AULSS n. 9 Scaligera.

Obiettivo del Security Assessment è di stabilire lo stato di sicurezza del sistema informatico, verificando, ad esempio, che l'applicazione/sistema non contenga vulnerabilità che consentono di (lista non esaustiva):

- accedere ad informazioni secondo modalità che non rispettano le policy e i requisiti di sicurezza (ad esempio, che non vi siano accessi ad informazioni aggirando i sistemi di autenticazione).
- ottenere privilegi più ampi di quelli che sono stati assegnati dagli amministratori (ad esempio, passare da utente standard ad amministratore).
- interrompere il servizio (ad esempio mediante sostituzione/modifica delle componenti dell'applicazione).
- arrecare danni o violare altri sistemi aziendali (ad esempio sfruttando la vulnerabilità per attaccare altri sistemi);
- modificare il servizio per danneggiare la reputazione aziendale (ad esempio sostituendo la pagina principale di un portale pubblico).

AULSS n. 9 Scaligera si riserva la possibilità di effettuare un Assessment prima dell'avvio del servizio in produzione.

I Security Assessment consistono in generale di due attività:

- VA (Vulnerability Assessment): verifica infrastrutturale o applicativa volta all'identificazione delle vulnerabilità informatiche note
- PT (Penetration Test): attività che viene svolta dal punto di vista dell'attaccante con cui si cerca di capire come poter accedere all'asset in esame o alle informazioni in esso contenute sfruttando le

vulnerabilità presenti. In funzione dell'applicazione, i test sono rivolti a verificare l'eventuale sussistenza di rischi di natura differente.

- o Nel caso di applicazioni web, ad esempio, le vulnerabilità che vengono testate sono almeno quelle indicate dalla lista OWASP Top 10 Application Security Risks ([www.owasp.org](http://www.owasp.org)).
- o Nel caso generale di sviluppi software potranno essere applicabili a titolo esemplificativo i rischi presentati nella lista CWE/SANS TOP 25 Most Dangerous Software Errors (<https://www.sans.org/top25-software-errors/>) Se la soluzione proposta prevede di essere raggiunta attraverso le applicazioni mobili, questa non deve essere influenzata dalle vulnerabilità più comuni in questo tipo di software. Si prega di fare riferimento all'ultima versione disponibile di "OWASP TOP 10 Mobile Risks" ([www.owasp.org](http://www.owasp.org)).
- o Se la soluzione proposta prevede di essere raggiunta attraverso le applicazioni mobili, questa non deve essere influenzata dalle vulnerabilità più comuni in questo tipo di software. Si prega di fare riferimento all'ultima versione disponibile di "OWASP TOP 10 Mobile Risks".
- o In funzione del tipo di applicativo e del rischio, potranno essere eseguiti altri test per individuare altre vulnerabilità non indicate da OWASP o nuove vulnerabilità segnalate e individuate dai vari istituti internazionali (zero-day).

Al termine dei test sarà condiviso il risultato tramite il Report di Security Assessment con i risultati ottenuti. Resta inteso che le vulnerabilità emerse e riconducibili o introdotte dal Fornitore saranno risolte dal Fornitore stesso senza costi o oneri aggiuntivi per AULSS n. 9 Scaligera nel più breve tempo possibile e nel rispetto delle tempistiche di avvio del servizio o, se in costanza di servizio, secondo una pianificazione concordata con AULSS n. 9 Scaligera sulla base del livello di rischio complessivo associato a ciascuna vulnerabilità.

Le vulnerabilità valutate di alto rischio riscontrate prima del rilascio in produzione del sistema dovranno essere risolte prima della messa in produzione dello stesso. Le restanti vulnerabilità valutate con rischio medio e basso, a seguito di una valutazione dei rischi da parte della funzione Cybersecurity di AULSS n. 9 Scaligera e secondo indicazione di quest'ultima, potranno essere risolte entro tre mesi dal rilascio.

Nel caso di vulnerabilità riscontrate sul sistema già rilasciato in esercizio, la risoluzione delle vulnerabilità ad alto rischio deve essere effettuata nel più breve tempo possibile e in ogni caso entro un mese solare. Per le vulnerabilità a rischio medio e basso deve essere concordata tra le parti una pianificazione con le tempistiche di risoluzione considerando, tranne casi eccezionali, una tempistica massima di tre mesi per la mitigazione delle vulnerabilità a rischio medio e una tempistica analoga o in linea con le successive release di prodotto per le vulnerabilità a rischio basso.

Una volta che il Fornitore dichiara la risoluzione delle vulnerabilità, AULSS n. 9 Scaligera si riserva di effettuare un nuovo Security Assessment/Penetration Test per verificare l'effettiva risoluzione delle stesse. Qualora alcune vulnerabilità dichiarate risolte non dovessero risultare corrette, AULSS n. 9 Scaligera valuterà di applicare un addebito come contributo per le spese sostenute per il re-test, per un importo forfettario pari a x.000 (xmila) euro, salvo ulteriori addebiti da definirsi legati ad eventuali spese per la messa in disponibilità dell'ambiente di test.

Il mancato adempimento degli obblighi di mitigazione delle vulnerabilità o della pianificazione concordata con AULSS n. 9 Scaligera nei tempi previsti può determinare l'applicazione delle penali o sanzioni amministrative, se previste nel contratto tra le parti, salva ogni più ampia riserva di rivalsa legale per il diritto di risarcimento del danno.