S1.1-2

POLITICA DELLA QUALITA' E SICUREZZA DELLE INFORMAZIONI PER I FORNITORI

(UNI EN ISO 9001:2015 - UNI CEI EN ISO/IEC 27001:2024 - UNI CEI EN ISO/IEC 27017:2021)

Ver.4	02/11/2026	FG	MT	CEO	Confidenziale
REVISIONE	DATA	REDATTO	VERIFICATO	APPROVATO	RISERVATEZZA

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

Sommario

1 INTRODUZIONE....3

2 GENERALITÀ....3

2.1 RUOLI E RESPONSABILITÀ....3
2.2 CLASSIFICAZIONE DEI FORNITORI....3
2.3 RIESAME DEL FORNITORE....4
2.4 COMUNICAZIONE CON IL PERSONALE INTERNO....4
2.5 ESTENSIONE ALLA PRIVACY....4
2.6 CONDIVISIONE DELLA POLITICA CON I FORNITORI....4

3 FLUSSO GESTIONE FORNITORI....5

3.1 FLUSSO PER FORNITORI NON CLOUD....6
3.2 FLUSSO PER FORNITORI CLOUD....7

4 ALLEGATO 1 – REGISTRO DI VALUTAZIONE FORNITORI DI BENI E SERVIZI NON CLOUD....10

5 ALLEGATO 2 – REGISTRO DI VALUTAZIONE FORNITORI DI SERVIZI CLOUD....12

6 ALLEGATO 3 – RISCHI PER LA SICUREZZA DELLE INFORMAZIONI RELATIVI ALLA FORNITURA PRODOTTI E SERVIZI E PER IL GDPR....14

7 ALLEGATO 4 – LINEE GUIDA DEFINIZIONE CLAUSOLE PER LA SICUREZZA DELLE INFORMAZIONI....15

7.1 LINEE GUIDA PER I CONTRATTI DI FORNITURA....15
7.2 LISTA DEI CONTROLLI NEI CONTRATTI DI FORNITURA....16

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

1 Introduzione

Per sviluppare il suo business l'azienda è sempre più integrata in **catene di fornitura** in cui la componente digitale di HW, SW e connessioni di rete è sempre più preponderante.

Inoltre, poiché **sempre più dati vengono elaborati e archiviati in comune tra l'azienda e terze parti** (fornitori, partner, consulenti, clienti, ecc. ...) la protezione di tali dati che non sono direttamente sotto il controllo unico del "proprietario" è un problema sempre più significativo.

Nell'ambito del SGI si è definito il presente documento che descrive in dettaglio i requisiti e la politica per la qualità e la sicurezza delle informazioni nei rapporti dell'azienda con i fornitori, con riferimento ai requisiti delle norme ISO9001:2015, ISO/IEC 27001:2022 e ISO/IEC 27017:2015 per i servizi in cloud.

Gli obiettivi della linea guida sono:

- **avere una gestione di qualità dei fornitori, secondo le esigenze aziendali,**
- **fare in modo che sia l'azienda che i propri fornitori sappiano come gestire la sicurezza delle informazioni che vengono loro affidate,** in base al relativo livello di classificazione e secondo le loro aspettative e gli agreement definiti: ed inoltre siano consapevoli del proprio ruolo e dei requisiti da soddisfare in caso di incidente e crisi, per garantire la prontezza ICT per la *business continuity*, in conformità alle norme.
- **stabilire una linea guida chiara per la definizione e gestione dei contratti con i fornitori**, promuovendo trasparenza, responsabilità e sicurezza delle informazioni aziendali.

Per garantire il raggiungimento dell'obiettivo, l'ambito della politica **comprende anche i requisiti di sicurezza delle informazioni durante la fase di prevendita:** richiesta delle offerte, la preparazione, la sottoscrizione e la conferma/modifica delle aspettative del contratto.

2 Generalità

2.1 Ruoli e responsabilità

Il processo di gestione dei fornitori è in carico al Procurement Manager (PM) che si avvale del supporto tecnico del SSI per la valutazione degli aspetti tecnici, analisi criticità e analisi del rischio.

Il Procurement Manager ha la responsabilità di tenerli aggiornati a fronte di qualsiasi modifica delle forniture, delle condizioni tecnico economiche e di security, dei contratti o del livello di classificazione di criticità delle informazioni ed ha la responsabilità di notificare al Management Team eventuali criticità.

2.2 Classificazione dei fornitori

La gestione dei fornitori viene fatta, suddividendo **i fornitori in due categorie,** registrando i dati nel registro fornitori gestito su Aegis – modulo Fornitori, suddiviso in due sezioni**:**

- **fornitori di beni e servizi non cloud: sezione Fornitori non-cloud (generali)**

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

- **fornitori di servizi in cloud: sezione Fornitori cloud**

La gestione del registro è in carico al responsabile approvvigionamento PM.

La struttura delle due sezioni è riportata negli ALLEGATI 1 e 2 del documento.

2.3 Riesame del fornitore

Durante i processi di **audit interno** e di **riesame della direzione** saranno riesaminate le prestazioni dei fornitori registrate e definite eventuali azioni migliorative.

2.4 Comunicazione con il personale interno

È fondamentale che tutti i dipendenti coinvolti nel processo di qualifica, definizione dei requisiti di fornitura e gestione del fornitore conoscano e rispettino la procedura.

L'azienda definisce all'interno del SGI **le modalità di comunicazione interne verso il personale.**

Per contratti di fornitura relative alle specifiche funzioni, l'azienda informerà tali funzioni circa le regole fissate dal contratto. In caso di contratti di fornitura inerenti tutto il personale sarà utilizzato il canale di comunicazione "bacheca elettronica".

Il canale di comunicazione è utilizzato per:

- Informare sulle definite (ed eventualmente fissate nel contratto) modalità e di scambio delle informazioni con i fornitori
- informare il proprio personale circa l'uso e la manutenzione del prodotto acquistato.
- informare il proprio personale circa l'utilizzo di servizi esternalizzati
- definire e monitorare le regole di controllo degli accessi dei fornitori ai sistemi ICT dell'impresa.
- definire e monitorare l'accesso fisico dei fornitori/*outsourcer* alle strutture, come avviene per i visitatori.

2.5 Estensione alla privacy

Qualora il fornitore abbia accesso alle informazioni di identificazione personale (PII) e la necessità di gestirle, viene richiesto il rispetto del GDPR in qualità di Responsabile del trattamento, mediante nomina ai sensi dell'art. 28 del GDPR (DPA). Tutte queste regole dovranno essere applicate nel caso in cui le informazioni personali vengano gestite da (o scambiate con) un fornitore/*outsourcer*, in conformità al GDPR.
Le modalità di gestione sono definite nel documento D2.2-4 – Gestione aziendale GDPR.

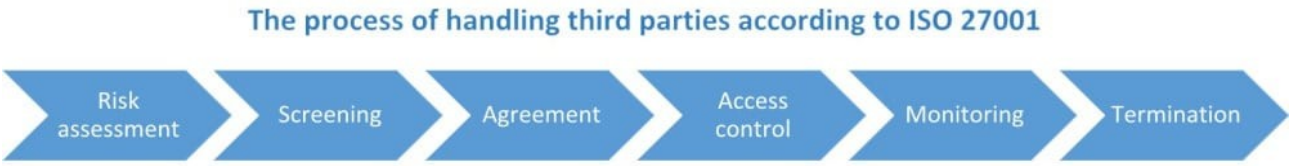
2.6 Condivisione della politica con i fornitori

Il presente documento viene condiviso con i fornitori che richiedono valutazione (criticità ≥ 3) all'avvio del rapporto e a ogni nuova versione. L'avvenuta condivisione è registrata nel campo "Politica Q&SI condivisa" del registro fornitori su Aegis.

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

3 Flusso gestione fornitori

La gestione dei fornitori viene implementata compilando i dati delle due sezioni del registro fornitori su Aegis, che sono stati definiti secondo il processo descritto dal seguente flusso:



Il processo include le fasi:

1. **RISK ASSESSMENT: valutazione del rischio di sicurezza**

   I partner della *catena di fornitura* possono essere soggetti a determinati rischi di minacce e vulnerabilità che, qualora si verifichi un evento che coinvolga le parti, potrebbero pregiudicare l'intera catena o una sua parte, con impatti che potrebbero essere estremamente diversi. È necessario quindi eseguire una valutazione del rischio e sulla base dei risultati di questa *risk analysis* si definisce come proseguire nei passaggi successivi di questo processo.

2. **SCREENING: valutazione dei fornitori**

   Sulla base dell'analisi dei rischi, viene eseguito uno screening dei fornitori esistenti e potenziali. Tali *controlli di background* saranno più approfonditi, maggiore è l'impatto dei rischi identificati sulle attività del fornitore nei confronti dell'azienda.

   Potrebbe essere necessario anche il controllo della reputazione dei fornitori mediante l'acquisizione di informazioni finanziarie e camerali dell'azienda, entro i limiti di legge.

   Per fornitori di servizi cloud le modalità e tecniche disponibili variano notevolmente: dall'analisi esterna degli attributi critici della SI relativi ai fornitori, alla verifica di dettaglio dei controlli e processi di sicurezza delle informazioni dei fornitori esistenti e delle loro competenze, anche mediante attività di audit.

3. **AGREEMENT: stipulazione degli accordi di sicurezza**

   Nel momento in cui sono noti quali sono i rischi di un servizio (RISK ASSESSMENT) e quale è la situazione specifica (SCREENING) dell'azienda scelta come fornitore/partner, si valuta la necessità e la possibilità della definizione e sottoscrizione di clausole di AGREEMENT.

4. **ACCESS CONTROL: accessi ai dati consentiti**

   Per ciascun fornitore integrato nella catena di fornitura con impatto sulla sicurezza delle informazioni dell'Azienda, viene definito a quali dati, in che modalità e con quali controlli, viene consentito l'accesso ai dati aziendali, sulle basi dei principi del "*Need-to-know*" e del *minimo privilegio* (accesso solo ai dati necessari per svolgere il loro lavoro).

5. **MONITORING: monitoraggio della conformità**

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

Viene verificato che il fornitore abbia accettato l'eventuale l'agreement condiviso. Viene monitorato il rispetto delle clausole di SLA e di sicurezza delle informazioni dell'accordo stipulato, sia da parte del fornitore (se opportuno e possibile, anche mediante audit) che dell'azienda.

6. **TERMINATION: terminazione con restituzione asset**
   In caso di terminazione del contratto di fornitura, l'Azienda deve assicurarsi che tutti i beni vengano restituiti (restituzione ed eliminazione dati dal servizio cloud) e che tutti i diritti di accesso vengano rimossi.

Questo processo, oltre a rispondere alla ISO 9001:2015 (§8.4), fa riferimento ai controlli della ISO/IEC 27001:2022: A.5.19, A.5.20, A.5.21, A.5.22, A.5.23 (servizi cloud) e A.6.1 (applicato ai fornitori); A.5.18 e A.8.3 (per l'ACCESS CONTROL informatico applicato ai fornitori e la rimozione degli accessi in caso di TERMINAZIONE); A.5.11 (per la restituzione di asset e dati in caso di TERMINAZIONE); oltre ai controlli della ISO/IEC 27017 per i servizi cloud.

3.1 FLUSSO PER FORNITORI NON CLOUD

Per i fornitori di prodotti e servizi non cloud, il flusso viene applicato mediante la sezione Fornitori non-cloud (generali) del registro fornitori su Aegis.

In questo caso viene sempre eseguito lo **SCREENING: VALUTAZIONE PARAMETRI MANDATORI:**

- Tempi di fornitura.
- Qualità del servizio offerto.
- Rapporto qualità/costi.
- SLA rispondenti ai requisiti.
- Gestione problemi e incidenti

I parametri mandatori determinano il Punteggio Qualità del fornitore e non concorrono alla media di adeguatezza per la sicurezza delle informazioni.

Mentre, sulla base della analizzata **CRITICITA' AZIENDALE DEL SERVIZIO OFFERTO (RISK ASSESSMENT),** fatta a due livelli:

- **Criticità SI** - criticità acquisita dall'impatto delle informazioni gestite**,** pari al valore massimo, per ciascuna dimensione DCIA, delle informazioni a cui il fornitore accede (Aegis – modulo Asset e Informazioni)
- **Criticita C** - criticità intrinseca del fornitore stesso basata sull'impatto potenziale che il fornitore può avere su qualità del prodotto/servizio finale e continuità operativa, e sul sistema di gestione della qualità aziendale, valutata dal PM.

viene determinata (valutazione richiesta quando almeno una delle due criticità è ≥ 3) la necessità o meno dello **SCREENING: VALUTAZIONE PARAMETRI DI CRITICITA':**

- Certificazione del fornitore
- Responsabilità GDPR
- Documentazione disponibile e comunicazione
- Sviluppo Sicuro

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

dove il fornitore viene valutato sulla base di punteggi che consentono di definire una **VALUTAZIONE TOTALE parametrica**, dalla quale si classifica il fornitore in quattro categorie:

- - fornitore da evitare (rosso)
- - fornitore accettabile solo per processi a criticità bassa (arancio)
- - fornitore adeguato (giallo)
- - fornitore eccellente, adatto a processi critici (verde)

e si determina la sua idoneità al servizio offerto e la necessità o meno di un **AGREEMENT** formale. Documenti con tali clausole di AGREEMENT, se presenti, vengono riferiti nel campo AGREEMENT della sezione Fornitori non-cloud.

Per gli **ACCESS CONTROL** viene riportato se il fornitore ha accesso informatico a dati dell'azienda, mediante accesso alle piattaforme software, specificando in questo caso: i criteri, le modalità di gestione e controllo e le limitazioni.

Il **MONITORAGGIO DELLA CONFORMITA'** viene eseguito su base semestrale e in caso di cambiamenti dal responsabile approvvigionamento PM che porta eventuali aggiornamenti alle informazioni riportate nel registro fornitori su Aegis.
Alla chiusura del contratto di collaborazione con il fornitore, vengono registrate le operazioni di **TERMINAZIONE DEL CONTRATTO CON RESTITUZIONE ASSET**.

3.2 FLUSSO PER FORNITORI CLOUD

Per i fornitori di servizi cloud, il flusso viene applicato mediante la sezione Fornitori cloud del registro fornitori su Aegis.

In questo caso, sulla base della **CRITICITA' AZIENDALE DEL SERVIZIO CLOUD OFFERTO (RISK ASSESSMENT),** ottenuta dall'analisi dei rischi su tutti i tipi di informazioni gestite dal fornitore registrata su Aegis – modulo Asset e Informazioni, come definito nella linea guida ***"S4.2-1 – Linee guida per la gestione degli asset informatici"*** **.**

con il criterio riportato nella tabella:

Tipo di impatto	Criterio di valutazione dell'impatto della CRITICITA' AZIENDALE	Decisione
Medio o Alto	Per tutte le informazioni trattate dal fornitore, Il valore di rischio più alto dei quattro attributi è 3 o 4.	È necessario procedere alla fase successiva di SCREENING e AGREEMENT del fornitore
Basso o Nullo	Per tutte le informazioni trattate dal fornitore, Il valore di rischio più alto dei quattro attributi è 1 o 2	Non è necessario procedere alla fase successiva di SCREENING e di AGREEMENT del fornitore

viene determinata la necessità o meno dello **SCREENING: VALUTAZIONE PARAMETRI DI CRITICITA'** definiti per i servizi cloud:

Per tutti i fornitori cloud vengono inoltre sempre valutati i parametri mandatori "Qualità del servizio offerto" e "Rapporto qualità/costi", che determinano il Punteggio Qualità e non concorrono alla media di adeguatezza per la sicurezza delle informazioni.

- CERTIFICAZIONI
- RUOLI E RESPONSABILITA'

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

- LIVELLO DI SERVIZIO
- CRITTOGRAFIA DEI DATI
- BACKUP E RECOVERY
- AUDIT E LOGGING
- GDPR
- GESTIONE VULNERABILITA' E INCIDENTI
- CONTROLLI SUGLI ACCESSI
- GEOLOCALIZZAZIONE DATI
- PROTEZIONE DEI DATI E PROPRIETA'
- DOCUMENTAZIONE DISPONIBILE E COMUNICAZIONE
- SVILUPPO SICURO

dove il fornitore viene valutato sulla base di punteggi dei singoli controlli che consentono di definire una **VALUTAZIONE TOTALE parametrica**, dalla quale si classifica il fornitore in quattro categorie:

- - fornitore da evitare (rosso)
- - fornitore accettabile solo per processi a criticità bassa (arancio)
- - fornitore adeguato (giallo)
- - fornitore eccellente, adatto a processi critici (verde)

e si determina la sua idoneità al servizio offerto e la necessità o meno di un **AGREEMENT** formale. Documenti con tali clausole di AGREEMENT, se presenti, vengono riferiti nel campo AGREEMENT della sezione Fornitori cloud.

In alcuni casi, soprattutto con fornitori consolidati sul mercato, che forniscono ampia documentazione e con cui non è possibile un accordo diretto, può essere sufficiente la documentazione pubblica rilasciata dal fornitore. Mentre quando necessario e possibile, si selezionano le clausole di sicurezza che devono essere inserite nell'accordo, che possono spaziare dal controllo degli accessi, all'etichettatura delle informazioni riservate, fino alla necessità di corsi di sensibilizzazione e ai metodi di crittografia da utilizzare.

Riguardo all'**ACCESS CONTROL**, i tipi di dati a cui accedono i fornitori di servizi cloud sono definiti su Aegis – modulo Asset e Informazioni. Mentre le modalità di controllo applicate sono riportate nei PARAMETRI CRITICI, oggetto delle SCREENING.

Il **MONITORAGGIO DELLA CONFORMITA'** viene eseguito su base semestrale e in caso di cambiamenti dal responsabile approvvigionamento PM che porta eventuali aggiornamenti alle informazioni riportate nel registro fornitori su Aegis.

Alla chiusura del contratto di collaborazione con il fornitore, vengono registrate le operazioni di **TERMINAZIONE DEL CONTRATTO CON RESTITUZIONE ASSET**.

Nell'ALLEGATO 4 sono riportate le linee guida per definire le clausole di sicurezza delle informazioni nei contratti di fornitura.

A ciascuno di questi controlli dei PARAMETRI DI CRITICITA' corrispondono specifici requisiti della ISO/IEC 27017:2015.

Nell'ALLEGATO 3 sono riportati i principali rischi dell'Azienda per la sicurezza delle informazioni relativi alla fornitura prodotti e servizi e per il GDPR.

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

4 Allegato 1 – Registro di valutazione fornitori di beni e servizi non cloud

Il registro generico di valutazione fornitori viene gestito nella sezione Fornitori non-cloud (generali) del registro fornitori su Aegis, dove per ogni fornitore si gestiscono i seguenti gruppi di dati.

1. ANAGRAFICA FORNITORE
2. STATO ATTUALE
3. CRITICITA' SERVIZI OFFERTI
4. A - SCREENING: VALUTAZIONE PARAMETRI MANDATORI
   B - SCREENING: VALUTAZIONE PARAMETRI DI CRITICITA' (se applicabili)
5. VALUTAZIONE TOTALE
6. AGREEMENT
7. POLITICA Q&SI CONDIVISA
8. CONTROLLI ACCESSI AI DATI: ISO/IEC 27001
9. TERMINATION

n	Gruppo dati	Dati	Note
1	**ANAGRAFICA FORNITORE**	- **ID** (numero) - **Nome** - **Descrizione** - **Tipo servizi offerti** - **Data inizio rapporto**	
2	**STATO ATTUALE**	- **Stato (*)** - **Note**	STATO: ATTIVO, NON ATTIVO, POTENZIALE
3	**CRITICITA' AZIENDALE SERVIZI OFFERTI** **(1- RISK ASSESSMENT)**	- **Criticità SI (Sicurezza informazioni)** - **Criticità C (Complessiva qualità)** - **Richiede valutazione** - **Note**	**Criticità SI = (Sicurezza delle Informazioni) massimo valore DCIA delle informazioni trattate (Aegis – modulo Asset e Informazioni)** **Criticità C** = Complessiva, definita dal responsabile degli acquisti; considera l'impatto potenziale che il fornitore può avere su: qualità del prodotto/servizio finale e continuità operativa. CRITERI VALUTAZIONE: (4)(3) Medio-Alta criticità: Fornitori strategici e/o con accesso a dati di dipendenti e/o aziendali sensibili (2)(1) Bassa criticità: Fornitori non particolarmente strategici e/o accesso a dati non/poco sensibili **Richiede valutazione: SI se almeno una delle due criticità è ≥ 3**
4 a	**SCREENING: VALUTAZIONE PARAMETRI MANDATORI** **(2-SCREENING)**	**TEMPI DI FORNITURA** - **Tempi di fornitura** - **Note / Documento / Fonte** - **Punteggio tempi (*)**	**Tempi di fornitura**: (3) Tempi rapidi, (2) Tempi nella media, (1) Tempi bassi
		QUALITA' DEL SERVIZIO - Qualità del servizio offerto **Note / Documento / Fonte** - **Punteggio qualità (*)**	**Qualità del servizio:** (3) Alta qualità, (2) Media qualità, (1) Bassa qualità
		RAPPORTO QUALITA' COSTI - Rapporto qualità/costi. - **Note / Documento / Fonte** - **Punteggio qualità/costi (*)**	**Rapporto qualità/costi:** 3) Ottimo rapporto Q/C, (2) Buon rapporto Q/C, (1) Pessimo rapporto Q/C

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

		LIVELLO SERVIZIO SLA **- SLA SI/NO** **- Note / Documento / Fonte** **- Punteggio SLA***	**Punteggio SLA:** **(**3) Soddisfacente e in linea con quanto atteso (risposta entro 24 ore) (2) Soddisfacente (risposta entro pochi giorni) (1) Insoddisfacente (0) Non specificato
		GESTIONE PROBLEMI E INCIDENTI **- Gestione problemi e incidenti** **- Note / Documento / Fonte** **- Punteggio gest. incidenti (*)**	**Punteggio gest. Incidenti:** (3) Positiva (2) Mediocre (1) Carente (0) non valutabile
4 b	**SCREENING: VALUTAZIONE PARAMETRI DI CRITICITA'** **(2-SCREENING)**	**CERTIFICAZIONI** **- Certificazioni in essere** **- Note / Documento / Fonte** **- Punteggio certificazioni**	**Punteggio certificazioni:** (3) ISO 9001 o equivalenti, ISO 27001, altro aderente al settore (2) Una certificazione aderente al ruolo (1) Nessuna
		GDPR **- Responsabilità GDPR** **- Note / Documento / Fonte** **- Punteggio GDPR (*)**	**Punteggio GDPR:** Nomina DPO e contratto (3), (2), solo informativa (1), nulla (0)
		DOCUMENTAZIONE E COMUNICAZIONE **- Documentazione disponibile e comunicazione** **- Note / Documento / Fonte** **- Punteggio doc.comunicaz.**	**Punteggio Doc. E comunicazione:** (3) Documentazione completa ed esaustiva e/o comunicazione rapida ed efficace (2) Documentazione presente, ma non esaustiva e/o comunicazione efficace (1) Documentazione poco accessibile e/o comunicazione farraginosa (0) Documentazione assente e/o comunicazione estremamente difficile
		SVILUPPO SICURO (FORNIT.SW) **- Sviluppo sicuro** **- Note / Documento / Fonte** **- Punteggio svil.sicuro**	**Punteggio svil.sicuro:** (3) Spiegato in modo esaustivo e/o supportato da certificazioni (2) Spiegato in modo vago (1) Qualche accenno (0) Assente
5	**VALUTAZIONE TOTALE** **(2-SCREENING)**	**- Punteggio totale (*)** **- Valutazione idoneità fornitore***	**Punteggio totale:** Minimo punteggio: 0 , Massimo: 3 **Valutazione idoneità fornitore:** < 1: fornitore da evitare 1-2: fornitore accettabile solo per processi a criticità bassa 2-2.5: fornitore adeguato > 2.5: fornitore eccellente, adatto a processi critici
6	**AGREEMENT CONTRATTUALE** **(3-AGREEMENT)**	**- Presente SI/NO** **- Note, data, documenti**	**Note, data, documenti:** vengono specificate eventuali condizioni, data e documento dell'agreement.
7	**CONTROLLI ACCESSI AI DATI: ISO/IEC 27001** **(4 – ACCESS CONTR.)**	**- Presente SI/NO** **- Note, data, documenti**	**Presente SI/NO: se il fornitore ha accesso informatico a dati dell'azienda mediante accesso a piattaforme**
8	**TERMINAZIONE** **(6 – TERMINATION)**	**- Restituzione dati SI / NO** **- Eliminazione dati SI/NO** **- Rimozione accessi Si / NO** **- Note, data, documenti**	**Note, data, documenti:** vengono specificate eventuali condizioni, data e documento della terminazione del servizio

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

5 Allegato 2 – Registro di valutazione fornitori di servizi cloud

Il registro di valutazione fornitori dei servizi cloud viene gestito nella sezione Fornitori cloud del registro fornitori su Aegis, dove per ogni fornitore si gestiscono i seguenti gruppi di dati.

1. ANAGRAFICA FORNITORE
2. STATO ATTUALE
3. CRITICITA' SERVIZI OFFERTI
4. PARAMETRI SEMPRE RICHIESTI (QUALITÀ DEL SERVIZIO, RAPPORTO QUALITÀ/COSTI)
5. VALUTAZIONE PARAMETRI CRITICI
6. VALUTAZIONE TOTALE
7. AGREEMENT
8. POLITICA Q&SI CONDIVISA
9. TERMINATION

n	Gruppo dati	Dati	Note
1	**ANAGRAFICA FORNITORE**	**- ID** (numero) **- Nome** **- Descrizione** **- Tipo servizi offerti** **- Data inizio rapporto**	
2	**STATO ATTUALE**	**- Stato** **- Note**	**Stato**: ATTIVO, NON ATTIVO, POTENZIALE
3	**CRITICITA' AZIENDALE SERVIZI OFFERTI (1- RISK ASSESSMENT)**	**- Criticità servizi** - **Richiede valutazione** **- Note**	**Criticità: basata sul valore massimo delle informazioni trattate (risk assessment) registrate su Aegis – modulo Asset e Informazioni** **Richiede valutazione**: se il fornitore ha criticità 3 o 4 è richiesta la VALUTAZIONE PARAMETRI CRITICI o un agreement dedicato
4	**VALUTAZIONE PARAMETRI CRITICI (2-SCREENING) (4 – ACCESS CONTR.)**	**CERTIFICAZIONI** **- Certificazioni in essere** **- Note / Documento / Fonte** **- Punteggio certificazioni**	**Punteggio certificazioni:** ISO 27001, ISO 27017, ISO 9001 (3), Solo due (2), Solo una (1), Nessuna (0)
		RUOLI E RESPONSABILITA' **- Ruoli e Responsabilità** **- Note / Documento / Fonte** **- Punteggio**	**Punteggio**: Ruoli chiaramente documentati con responsabilità di sicurezza IT (3), Ruoli dichiarati ma senza dettaglio formale (2), Accenni vaghi (1), Assenti (0)
		LIVELLO DI SERVIZIO **- SLA** **- Note / Documento / Fonte** **- Punteggio SLA**	**Punteggio SLA: >** 99.99% (3), > 99.9% (2), > 99% (1), Non specificata (0)
		CRITTOGRAFIA DEI DATI **- Crittografia dei dati** **- Note / Documento / Fonte** **- Punteggio crittografia**	**Punteggio crittografia:** Dati in transit + at rest (3), solo at rest (2), solo in transit (1), nessuna (0)
		BACKUP E RECOVERY **- Backup e recovery** **- Note / Documento / Fonte** **- Punteggio Backup policy**	**Punteggio Backup policy:** Frequente e verificabile (3), Frequente ma non verificabile (2), Non Frequente e non verificabile (1), Assente o non specificato (0)
		AUDIT E LOGGING **- Audit e logging** **- Note / Documento / Fonte**	**Punteggio audit log:** Log accessibili e tracciati e auditabili (3), Log parziali o difficilmente reperibili (2),

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

		- Punteggio audit log	Log inaccessibili (1), Assenti (0)
		GDPR **- Responsabilità GDPR** **- Note / Documento / Fonte** **- Punteggio GDPR (*)**	**Punteggio GDPR:** Nomina DPO e contratto (3), (2), solo informativa (1), nulla (0)
		GESTIONE VULNERABILITA E INCIDENTI **- Gestione vulnerabilità incidenti** **- Note / Documento / Fonte** **- Punteggio gest. Vuln. incidenti**	**Punteggio gest. Vuln. Incidenti:** Piano condiviso (3), (2), solo interno (1), assente (0)
		CONTROLLI SUGLI ACCESSI **- Controllo accessi** **- Note / Documento / Fonte** **- Punteggio contr. accessi**	**Punteggio contr. accessi:** MFA + RBAC (3), Solo uno dei due (2), accesso con solo password (1), aperto (0)
		GEOLOCALIZZAZIONE DATI **- Geolocalizzazione dati** **- Note / Documento / Fonte** **- Punteggio geolocal.**	**Punteggio Geolocal.:** EU o scelta (3), EU (2), NON EU (1), Non specificata (0)
		PROTEZIONE DEI DATI E PROPRIETA' **- Protezione dei dati e proprietà** **- Note / Documento / Fonte** **- Punteggio Protezione (*)**	**Punteggio Protezione:** Esplicita che i dati rimangono del cliente (3), Esplicita ma i dati possono essere usati per alcuni scopi (2), Esplicita, ma i dati possono essere usati per scopi non ben definiti (1), Non Definita (0)
		DOCUMENTAZIONE DISPONIBILE E COMUNICAZIONE **- Documentazione e comunicazione** **- Note / Documento / Fonte** **- Punteggio doc.comunicaz.**	**Punteggio doc. e comunicaz.:** Completa ed esaustiva (3), Non esaustiva (2), poco accessibile (1), assente (0)
		SVILUPPO SICURO **- Sviluppo sicuro** **- Note / Documento / Fonte** **- Punteggio Svil.sicuro**	**Punteggio Svil.sicuro:** Spiegato in modo esaustivo / supportato da certificazioni (3), Spiegato in modo vago (2) Qualche accenno (1), assente (0)
5	**VALUTAZIONE TOTALE (2-SCREENING)**	**- Punteggio totale** **- Valutazione idoneità fornitore**	**Punteggio totale:** Calcolo della media con valori, Minimo 0 e Massimo: 3 **Valutazione idoneità fornitore:** < 1: fornitore da evitare, 1-2: fornitore accettabile solo per processi a criticità bassa, 2-2.5: fornitore adeguato ma richiesti ulteriori audit e verifiche, > 2.5: fornitore eccellente, adatto a processi critici
6	**AGREEMENT (3-AGREEMENT)**	**- Presente SI/NO** **- Note, data, documenti**	**Note, data, documenti:** vengono specificate eventuali condizioni, data e documento dell'agreement.
7	**TERMINAZIONE (6 – TERMINATION)**	**- Restituzione dati SI / NO** **- Eliminazione dati SI/NO** **- Rimozione accessi Si / NO** **- Note, data, documenti**	**Note, data, documenti:** vengono specificate eventuali condizioni, data e documento della terminazione del servizio

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

6 Allegato 3 – Rischi per la sicurezza delle informazioni relativi alla fornitura prodotti e servizi e per il GDPR

Di seguito vengono definiti i principali rischi dell'Azienda relativi alle due diverse tipologie di fornitura - prodotti e servizi - e i rischi relativi al GDPR dei fornitori.

Rischi relativi all'acquisizione di prodotti

Nell'acquisizione di prodotti vengono considerati i seguenti rischi

- Alcune delle informazioni scambiate, necessarie al processo di fornitura potrebbero essere informazioni sensibili.
- La mancata conformità del prodotto fornito alle specifiche può influire sulla capacità dell'Azienda di eseguire le attività previste, soprattutto se si tratta di infrastrutture ICT critiche.
- Le vulnerabilità del prodotto possono pregiudicare il livello di sicurezza dell'Azienda
- Accesso del fornitore ai sistemi ICT e alle informazioni dell'Azienda può determinare delle criticità. Ad esempio, nel caso l'Azienda richieda il monitoraggio dei suoi processi di produzione o l'esternalizzazione di alcune operazioni

Rischi relativi all'acquisizione di servizi

Nell'acquisizione di servizi vengono considerati i seguenti rischi:

- Accesso del fornitore alle informazioni dell'Azienda. Ad esempio, nel caso di esternalizzazione, cloud, BU, manutenzione delle apparecchiature ICT, ecc. .
- Accesso del fornitore alle strutture dell'Azienda. Ad esempio, in caso di esternalizzazione di attività a personale del fornitore o per i servizi esterni come il servizio di pulizia (dove le attività avvengono molto spesso al di fuori dell'orario di ufficio e gli addetti alle pulizie hanno accesso a tutti gli spazi e ai locali dell'azienda).
- L'Azienda può (se necessario e possibile) richiedere il monitoraggio dei processi del fornitore per controllarne la qualità (e la sicurezza del servizio, ad esempio ai fini della conformità al GDPR).
- Utilizzo, da parte dei fornitori di servizi di intelligenza artificiale (es. modelli linguistici), dei dati trasmessi per finalità ulteriori, come l'addestramento dei modelli, o loro trattamento al di fuori dell'Unione Europea.

Rischi relativi al GDPR

- Rischi relativi all'accesso, luogo di archiviazione e conservazione delle informazioni di identificazione personale dell'acquirente.
- Rischi relativi alla catena di approvvigionamento del fornitore, qualora quest'ultimo esternalizzi parte delle proprie attività con diffusione dei dati dall'Azienda. In questo caso deve essere controllato che vengano implementate le medesime "regole di conformità" ai subfornitori.

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

7 Allegato 4 – Linee guida definizione clausole per la sicurezza delle informazioni

7.1 Linee guida per i contratti di fornitura

Nel seguito vengono definite **la politica e la lista dei controlli** da considerare nella definizione dei contratti di fornitura, per garantire una corretta gestione della sicurezza delle informazioni,

7.1.1.1 Politica di sicurezza delle informazioni nella gestione del contratto

Vengono definiti i seguenti **principi da rispettare** quando l'Azienda conclude, sottoscrive, adempie e risolve i contratti con i fornitori di prodotti e gli outsourcer dei servizi.

- I contratti devono essere **redatti e sottoscritti da una persona appartenente ai vertici aziendali.**
- **Lo scopo del contratto** deve essere chiaramente indicato; come, ad esempio, l'esigenza dell'acquirente di supportare le attività aziendali oppure attività specifiche che sono al di là delle sue competenze, ma essenziali per il raggiungimento degli obiettivi aziendali (ad esempio ICT).
- Devono sempre essere considerati **diversi tipi di elementi,** al fine di garantire la sottoscrizione di contratti affidabili:
  - informazioni relative all'azienda fornitrice, necessarie per adempiere il contratto sottoscritto;
  - aspettative e requisiti dell'approvvigionamento/fornitura dei beni e dei servizi oggetto del contratto;
  - aspettative e requisiti a supporto dell'Azienda in caso di incidente e crisi; regole da seguire in caso di conflitto durante il periodo di validità del contratto; clausole contrattuali e obblighi relativi al periodo di conservazione dei dati (aggiornamento o distruzione delle informazioni fornite/memorizzate).
  - fase di qualifica del fornitore che, a seconda del tipo di fornitura, può comprendere la verifica dei requisiti di sicurezza, fino alla possibilità di eseguire un audit per riscontrare il rispetto di questi requisiti.
  - definizione degli accordi di riservatezza con il fornitore.
  - certificazioni del fornitore: sarà valutato in modo preferenziale la certificazione del fornitore ISO 9001 e ISO/IEC27001 o equivalenti per altre aree geografiche.
- Devono sempre essere considerati **i criteri fondamentali della sicurezza delle informazioni**:
  - il principio del "privilegio minimo", in modo che il fornitore abbia accesso esclusivamente alle informazioni strettamente necessarie per adempiere il contratto.
  - La protezione riguardo l'accesso e il trasferimento di informazioni in base ai tre criteri di sicurezza - riservatezza, integrità e disponibilità – ed eventualmente l'autenticità.

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization

- Devono sempre essere considerati **le modalità necessarie a garantire questi criteri:**
  - Implementazione di buone pratiche e processi (ad esempio con un SGSI/ISMS, pratiche per GDPR, certificazioni e applicazione di standard, ...).
  - Controllo dell'accesso dei fornitori alle informazioni e alle strutture dell'acquirente.
  - Contratti sul livello del servizio (Service Level Agreement - SLA) e affidamento di incarico.
  - Accordi di riservatezza su informazioni critiche, personali e non personali.
- I contratti devono contenere clausole e allegati relativi alla sicurezza delle informazioni accettati da entrambe le parti, che prevedano **una serie di controlli e responsabilità** per quanto riguarda l'implementazione e il monitoraggio della sicurezza delle informazioni, **anche in caso di soluzioni contrastanti e di incidenti di sicurezza delle informazioni**, **compresi gli incidenti relativi alla privacy.**
- I contratti dovranno definire **i protocolli di scambio delle informazioni, da utilizzare qualora vengano condivise "Informazioni critiche protette".**

7.2 Lista dei controlli nei contratti di fornitura

La lista dei controlli a cui sottoporre i contratti con i fornitori devono contenere:

- clausole relativi alla sicurezza delle informazioni accettati da entrambe le parti in termini di disponibilità, confidenzialità, integrità e autenticità
- eventuali allegati relativi alla sicurezza delle informazioni accettati da entrambe le parti
- le responsabilità delle parti
- modalità di monitoraggio
- definizione degli SLA di servizio
- definizione di eventuali penali se previste
- accordi di riservatezza
- modalità di segnalazione e gestione degli incidenti, inclusi quelli sulla privacy
- i protocolli di scambio delle informazioni, da utilizzare qualora vengano condivise "Informazioni protette".

CONFIDENTIAL - This document is reserved for its intended recipients and may not be disclosed to third parties without written authorization