Requisiti minimi di sicurezza delle informazioni[1]

Sicurezza delle informazioni e gestione del rischio

[1] Il documento è disponibile al seguente indirizzo: https://www.novartis.com/about-us/corporate-responsibility/resources/codes-policies-guidelines/

Requisisti minimi di sicurezza delle informazioni[2]

1. Gestione e conformità

- Il fornitore è tenuto ad adottare policy e standard di sicurezza organizzativa allineati agli standard nel settore della sicurezza dell'informazione e a garantirne la conformità.
- Il fornitore deve incaricare una persona idonea quale responsabile ad assicurare la conformità tecnica e organizzativa con i requisiti di sicurezza e di privacy definiti nel presente contratto e nelle policy del fornitore.

2. Continuità del servizio

- Il fornitore deve disporre di adeguati piani di business continuity, tra cui piani di disaster recovery IT, per prevenire e/o garantire il ripristino tempestivo dei propri sistemi informatici che memorizzano o trattano i dati della società Novartis, o dei sistemi informatici che supportano in altro modo i servizi forniti a Novartis, in caso di disastro.
- Il fornitore è tenuto a garantire che questi piani di disaster recovery siano regolarmente testati e aggiornati per assicurarne l'attualità ed il corretto funzionamento.
- Il fornitore è tenuto a mantenere l'integrità e la disponibilità delle informazioni e degli strumenti utilizzati per il trattamento delle stesse tramite i backup delle informazioni e dei software, che devono essere eseguiti e testati regolarmente ed in conformità con le policy concordate per il backup.

3. Gestione dei supporti dati

- Il fornitore deve definire delle procedure di gestione e salvataggio delle informazioni, al fine di proteggere le informazioni stesse dalla divulgazione non autorizzata o dall'uso improprio.
- Il fornitore deve garantire che i supporti dati utilizzati per memorizzare le informazioni vengano smaltiti in modo sicuro quando non sono più necessari, seguendo delle procedure formali.
- Il fornitore garantisce che la documentazione di sistema sia protetta da accessi non autorizzati.

4. Scambio di informazioni

- Il fornitore è tenuto a mantenere la sicurezza delle informazioni e del software scambiati all'interno della propria organizzazione e con qualsiasi entità esterna; ciò include accordi relativi allo scambio, trasmissione dei supporti fisici di memorizzazione dati, la messaggistica elettronica e la protezione delle informazioni relative al collegamento dei sistemi informativi aziendali.

5. Controllo degli accessi

- Il fornitore è tenuto a definire e ad attuare politiche di controllo degli accessi per garantire l'accesso autorizzato agli utenti e impedire l'accesso non autorizzato, soprattutto ai dati personali sensibili.
- Il fornitore deve rivedere i diritti di accesso degli utenti al fine di garantire che l'assegnazione e l'utilizzo dei privilegi siano regolamentati e, se necessario, limitati.

[2] I termini utilizzati nel presente documento hanno lo stesso significato indicato nel codice dei fornitori della società Novartis (https://www.novartis.com/about-us/corporate-responsibility/resources/codes-policies-guidelines) se non sono esplicitamente definiti nel glossario dei termini allegato, se non diversamente specificato o se il contesto non richiede un'altra interpretazione.

6. Crittografia

- Nelle situazioni più rischiose, il fornitore deve integrare i controlli degli accessi con la crittografia, sia nel caso dei dati memorizzati, sia nel caso dei dati trasmessi. Il rischio aumenta in base a:
  - il tipo di dati (ad esempio, i dati personali sensibili o informazioni che possono avere un impatto significativo sulla società Novartis richiedono una protezione migliore rispetto ai dati che non sono personali o riservati)
  - vulnerabilità (ad esempio, i dati memorizzati in un sistema esposto sulla rete internet sono più vulnerabili rispetto ai dati memorizzati all'interno di una rete privata)
  - rischi correlati (ad esempio, i dati trasmessi tramite una rete aperta sono più a rischio).
- Il fornitore deve essere in possesso di policy relative all'uso della crittografia per la protezione delle informazioni, che devono essere implementate e rispettate.

7. Gestione della rete

- Il fornitore garantisce che le reti siano correttamente gestite, controllate e protette da minacce e garantisce la sicurezza dei sistemi e delle applicazioni che utilizzano la rete, comprese le informazioni su questa trasmesse.

8. Formazione e sensibilizzazione sulla sicurezza delle informazioni

- Il fornitore provvede affinché tutti i dipendenti, fornitori e utenti di terzi siano a conoscenza delle minacce e dei rischi relativi alla sicurezza delle informazioni, sui loro doveri e responsabilità e siano pronti a supportare le policy organizzativi e sulla sicurezza nel loro lavoro.
- Il fornitore provvede affinché dipendenti, fornitori e terzi che trattano i dati personali (compresi quelli codificati) conoscano la definizione di dati personali e dati personali sensibili riportata dalla Commissione europea e da altre autorità competenti.
- Il fornitore provvede affinché, se necessario, tutti i dipendenti, fornitori e utenti di terze parti ricevano adeguata formazione in merito.
- Il fornitore provvede affinché i suoi dipendenti utilizzino indirizzi di posta elettronica aziendale per la comunicazione o la trasmissione di dati e/o informazioni personali.

9. Sicurezza fisica e sicurezza dell'ambiente

- Il fornitore provvede affinché siano implementati appropriati perimetri di sicurezza e controlli sugli accessi, al fine di prevenire accessi fisici non autorizzati, danni e interferenze nei locali e alle informazioni del fornitore, compresi tutti i dispositivi degli utenti finali.
- Il fornitore garantisce che le proprie apparecchiature siano mantenute regolarmente al fine di assicurarne la disponibilità e l'integrità.

10. Protezione dei dati dell'organizzazione

- Il fornitore deve garantire che le sue policy di sicurezza includano principi per la conservazione, la distruzione e standard di sicurezza dei dati.
- Il fornitore assicura l'implementazione di controlli al fine di prevenire la perdita, la distruzione o la falsificazione di dati informatici durante il periodo di conservazione.
- Su richiesta di Novartis o dopo la risoluzione del contratto, il fornitore si impegna a dismettere (ad esempio, eliminando, distruggendo o rendendoli illeggibili) tutti i dati della società Novartis di cui dispone il fornitore, i suoi affiliati o subappaltatori (ad eccezione di eventuali copie dei dati Novartis su supporti di backup standard del fornitore, a condizione che tali supporti di backup siano protetti secondo le best practice nel campo della privacy e della sicurezza dei dati). Su richiesta di Novartis, il fornitore consegnerà alla società Novartis un report dettagliato che includa i dati memorizzati sul supporto di backup, senza che Novartis debba sostenere costi aggiuntivi.

- Su richiesta di Novartis, il fornitore dovrà fornire conferma per iscritto che le suddette azioni sono state effettuate.

- I seguenti casi sono eccezioni al presente requisito di distruzione:
  – Il fornitore è tenuto a memorizzare i dati di Novartis per scopi legali o regolamentari; questi dati di Novartis saranno rimossi una volta decorsi i termini legali di conservazione;
  – I dati di Novartis che quest'ultima ha richiesto al fornitore di preservare per eventuali contenziosi legali

11. Gestione delle vulnerabilità tecniche

- Il fornitore si adopera per ridurre i rischi derivanti dalle vulnerabilità tecniche note relative ai vari componenti dei propri sistemi informativi.
- Il fornitore implementerà le best practice di settore definite ad esempio negli standard CIS-Center for Internet Security (https://www.cisecurity.org/)

12. Gestione degli incidenti di sicurezza informatica

- Il fornitore deve assicurare la gestione delle responsabilità e procedure per garantire una reazione rapida, efficace e appropriata agli incidenti di sicurezza e la corretta gestione e segnalazione degli incidenti di sicurezza informatica e relativi punti deboli.

13. Monitoraggio

- Il fornitore utilizzerà sistemi di sicurezza adeguati per il controllo e la rilevazione di attività non autorizzate durante il trattamento delle informazioni.

14. Gestione della configurazione

- Il fornitore deve stabilire e mantenere delle policy per l'applicazione adeguata di aggiornamenti e patch dei sistemi.
- Il fornitore deve creare e mantiene un inventario del software e hardware utilizzato ed eseguire controlli regolari della vulnerabilità tecniche.
- Il fornitore deve implementare dei controlli di audit al fine di garantire la possibilità di effettuare degli audit/test indipendenti sui dati di produzione, riducendo al minimo il rischio di interruzione dei processi aziendali.

15. Prevenzione di malware

- Il fornitore deve redigere delle policy per regolamentare i rischi dei processi aziendali in relazione al codice malevolo, che includono anche l'implementazione di difese anti-malware.

16. Gestione dei rischi connessi all'informazione

- Il fornitore deve creare un framework che includa delle policy di gestione del rischio che consentano e supportino la gestione del rischio connesso all'informazione.

Glossario dei termini

"**Contratto**" indica qualsiasi accordo formale scritto, stipulato tra il fornitore e/o società collegate e la società Novartis e/o società affiliate, in cui si fa riferimento o è altrimenti integrato il codice dei fornitori dell'azienda Novartis (versione 3) (escludendo da questo scopo gli accordi di riservatezza che non prevedono alcuna produzione/fornitura di beni o servizi).

"**Società affiliata**" indica, salvo diversa definizione nell'ambito di un accordo speciale (nel qual caso l'espressione "società affiliata" verrà definita in detto accordo speciale), qualsiasi persona giuridica, azienda o società che controlla o è controllata dalla società Novartis direttamente o indirettamente (in questo caso si tratta di "società collegata alla società Novartis"), o che controlla o è controllata dal fornitore direttamente o indirettamente (in questo caso si tratta di "società collegata al fornitore"). Ai fini della presente definizione, la parola "controlla/controllata" indica, nelle diverse forme grammaticali, il possesso diretto o attraverso una o più affiliate di almeno il 50% delle azioni con diritto di voto per l'elezione dei dirigenti in caso di società per azioni, o almeno il 50% del capitale proprio per qualsiasi altro tipo di persona giuridica, lo stato di partner generale in caso di partnership o qualsiasi altro accordo in base al quale una parte controlla o ha il diritto di controllare il consiglio di amministrazione o un organo equivalente di società o altra persona giuridica, oppure la capacità di controllare la gestione o le strategie della società o di altra persona giuridica.