Apio Srl
Sede legale: Via dei Teatini, 12 - 65127 Pescara (PE) – ITALIA
Sede operativa 1: Via Salara, 20 - 66020 San Giovanni Teatino (CH) - ITALIA
Contatti: +39 085 9396500 - info@apio.cc - www.apio.cc
P.IVA e C.F.: IT02094420680 – Capitale sociale: 14.881,58 €
Numero REA: PE - 153248 – PEC: apio@pec.it
Iscritta nell'apposita sezione speciale in qualità di PMI innovativa

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

1 Introduzione

Oggigiorno le informazioni digitali sono sempre più esposte ad un crescente numero di minacce e vulnerabilità, ragion per cui ogni azienda che gestisce informazioni digitali di qualunque tipo e natura, deve adottare una Politica indirizza la gestione della sicurezza delle informazioni e seguire un piano di gestione degli incidenti di sicurezza informatica. La presente Politica per la sicurezza delle informazioni indirizza la gestione della sicurezza delle informazioni all'interno della società APIO Srl e di tutte le sue società partecipate, al fine di assicurare adeguati livelli di sicurezza per le informazioni (dati personali, dati finanziari, ecc.), memorizzate e trasmesse, attraverso strumenti e tecnologie informatiche, considerando anche tutti gli annessi rischi e la loro relativa gestione. La presente Politica per la sicurezza delle informazioni viene rivista formalmente almeno una volta ogni tre anni.

2 Scopo e obiettivi

Lo scopo del presente documento è quello di fornire una descrizione delle politiche di sicurezza adottate all'interno della società APIO Srl e di tutte le sue partecipate, per garantire un adeguato livello di protezione delle informazioni in termini di riservatezza, integrità e disponibilità delle stesse. Le politiche di sicurezza delle informazioni sono state definite in conformità agli standard internazionali (es. ISO/IEC 27001) e alle norme relative alle pratiche di gestione della sicurezza delle informazioni, agli aspetti e ai fattori di rischio così come da analisi riportata nel **Mod 610 - Valutazione Rischi e Piani di Trattamento** che caratterizzano la società APIO Srl.

3 Politica per la sicurezza delle informazioni

APIO Srl ha definito 4 domini di sicurezza da presidiare con apposite policy di sicurezza delle informazioni, che tutte le funzioni/strutture aziendali implementano e seguono. Le aree dei domini di sicurezza sono:

- Area controlli organizzativi
    - Ruoli e Responsabilità nella sicurezza delle informazioni
    - Gestione degli asset
    - Classificazione delle informazioni
    - Controllo degli accessi
    - Sicurezza delle informazioni nelle terze parti
    - Compliance
- Area controlli sul personale
    - Sicurezza delle Risorse Umane
- Area controlli fisici
    - Sicurezza fisica
    - Sicurezza ambientale

- Area controlli tecnologici
    - Sicurezza delle operazioni
    - Sicurezza delle comunicazioni
    - Gestione degli incidenti relativi alla sicurezza delle informazioni
    - Gestione della Business Continuity e Disaster Recovery

4 Controlli organizzativi

4.1.1 Ruoli e Responsabilità nella sicurezza delle informazioni

La Struttura ICT di APIO Srl è responsabile della sicurezza delle informazioni e della gestione dei rischi a questa correlati. La Struttura ICT si occupa di:

- Garantire lo sviluppo e l'assistenza sistemistica delle infrastrutture hardware;
- Garantire lo sviluppo e la gestione degli applicativi in uso;
- Supportare la Governance nella definizione e revisione delle strategie ICT nonchè per l'individuazione, sviluppo ed implementazione di nuove infrastrutture e/o soluzioni applicative adeguate alle esigenze espresse dalle diverse strutture e funzioni coerenti con gli obiettivi societari;
- Progettare, realizzare ed erogare, coordinandosi con la struttura Risorse Umane, il fabbisogno formativo sull'uso dei sistemi;
- Curare, per l'ambito di propria competenza ed in collaborazione con la struttura DL - QASE - Facility Management, la predisposizione e l'aggiornamento delle procedure operative, al fine di garantirne l'ottimale rispondenza agli standard qualitativi fissati normativamente o sulla base di obiettivi autonomamente adottati dalla società;
- Gestire il rischio di sicurezza delle informazioni, con la collaborazione di società esterne a APIO Srl, svolgendo valutazioni periodiche del rischio per identificare le priorità per la gestione dei rischi relativi alla sicurezza delle informazioni e per l'esecuzione dei controlli volti alla ridurre di tali rischi;
- Informare il Consiglio di amministrazione sui rischi di cyber security, proponendo strategie volte ad aumentare la sicurezza logica e fisica delle infrastrutture informatiche;
- Gestire/sovrintendere i fornitori che si occupano delle tematiche relative alla sicurezza delle informazioni;
- Stabilire con la collaborazione di società esterne a APIO Srl le politiche di sicurezza delle informazioni;
- Mantenere aggiornate, con la collaborazione di società esterne a APIO Srl, le procedure di sicurezza delle informazioni;
- Assicurare, grazie alla collaborazione di società esterne, attraverso valutazioni periodiche, l'efficacia delle misure di sicurezza delle informazioni al fine di proteggere il patrimonio aziendale e garantire il rispetto delle norme relative alle pratiche di gestione della sicurezza delle informazioni e dei requisiti aziendali;

- Eseguire attività di controllo della sicurezza delle informazioni sulla catena di fornitura e su altre terze parti rilevanti;
- Supportare li ove possibile e con la collaborazione di società esterne a APIO Srl le attività di controllo della sicurezza delle informazioni richieste da terze parti;
- Gestire la progettazione di soluzioni appropriate per la sicurezza delle informazioni;
- Fornire supporto nelle attività di rilevamento e risposta agli incidenti di sicurezza delle informazioni;
- Assicurare il necessario supporto sugli aspetti normativi e legali in ambito sicurezza delle informazioni;
- Fornire indicazioni e partecipare alle attività di revisione delle politiche e dei regolamenti di sicurezza IT.

4.1.2 Gestione degli asset

Tutti gli asset (hardware/software e risorse di rete) associati alle informazioni **sono identificati e registrati in un inventario mantenuto aggiornato**. (MOD-630 Gestione delle infrastrutture)

Le regole per l'utilizzo degli asset sono documentate (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT) al fine di garantirne il corretto e sicuro funzionamento e per ridurre e prevenire i rischi (inclusi attacchi informatici, compromissione di sistemi e servizi di rete, questioni legali, ecc.) legati ad un uso inappropriato. I dipendenti e gli utenti esterni che utilizzano o hanno accesso agli asset aziendali sono resi consapevoli dei requisiti di sicurezza e responsabili di ogni utilizzo delle risorse informatiche aziendali, attraverso il suddetto regolamento, comunicato a tutti gli interessati attraverso i canali aziendali, nonché attraverso la formazione in ambito digitale (Mod 710b - Programma annuale formazione).

Tutti i dipendenti e gli utenti esterni devono restituire tutti i beni aziendali loro concessi al termine del rapporto di lavoro, del contratto o dell'accordo di collaborazione. La restituzione degli asset avviene tramite firma di apposita modulistica (Mod 811e - Modulo restituzione asset).

4.1.3 Classificazione delle informazioni

Tutti i dati hanno un **owner responsabile della loro classificazione**. Le procedure per il trattamento degli asset sono sviluppate e implementate in accordo con lo schema di classificazione delle informazioni adottato da APIO Srl (PROC-750 - Informazioni documentate).

4.1.4 Controllo degli accessi

Le informazioni sono protette dall'accesso non autorizzato per garantirne la riservatezza, l'integrità e la disponibilità. L'intero ciclo di vita delle utenze (creazione dell'account utente, cambiamento dell'account utente e rimozione dell'account utente) è definito per ridurre il rischio di accesso non autorizzato alle informazioni (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT). Inoltre, sono definiti i requisiti specifici sulla robustezza della password (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT) e le altre tecniche di autenticazione.

L'accesso remoto è limitato al personale autorizzato ed eseguito attraverso canali criptati utilizzando un appropriato processo MFA (Multi-Factor Authentication). I profili di accesso sono coerenti con le attività che devono essere svolte e **sono approvati dai rispettivi responsabili di area e/o funzione con comunicazione formale a mezzo mail**. Le attività di revisione periodica dei privilegi di accesso degli utenti vengono eseguite per tutti i sistemi informativi. Le autorizzazioni per i diritti di accesso privilegiati vengono riviste a intervalli più frequenti, in relazione alla criticità dei sistemi a cui si accede.

4.1.5 Sicurezza delle informazioni nelle terze parti

In caso di accesso di terze parti alle informazioni di APIO Srl, sono stabilite adeguate misure di sicurezza per garantire la riservatezza, l'integrità e la disponibilità delle informazioni, e gli accessi **sono approvati dai rispettivi responsabili di area e/o funzione con comunicazione formale a mezzo mail**. Gli accordi con le terze parti includono requisiti relativi alla protezione dei dati della società. In particolare, le terze parti devono essere disponibili a condividere, su richiesta, i loro piani di sicurezza, le misure di sicurezza implementate e relativa autocertificazione di compliance alle vigenti normative (Mod 840e - Accordo di non divulgazione e non utilizzo pre-affidamento; Mod 840f - Autocertificazione; Mod 840g - Accordo di non divulgazione e non utilizzo in esecuzione).

4.1.6 Compliance

La gestione dei sistemi informativi adottati in APIO Srl, è conforme alle leggi (es. GDPR), agli standard e alle politiche aziendali per prevenire i rischi di non conformità e le relative conseguenze (es. sanzioni, danni di reputazione, penali contrattuali, ecc.) **(Mod 610 - Valutazione Rischi e Piani di Trattamento).**

4.1.7 Controlli sul personale

4.1.8 Sicurezza delle Risorse Umane

Durante il processo di assunzione di personale, le attività di verifica effettuate dalla struttura Risorse Umane sui candidati sono proporzionate ai requisiti aziendali, alla classificazione delle informazioni a cui tali candidati potranno/dovranno accedere e ai relativi rischi associati.

Gli accordi contrattuali con i dipendenti e i collaboratori specificano **le loro responsabilità in tema di sicurezza delle informazioni (REG 01_REGOLAMENTO SULLE MODALITÀ DI UTILIZZO RISORSE ICT)**. I responsabili di struttura/funzione richiedono a tutti i dipendenti e collaboratori di applicare le misure di sicurezza in conformità con le politiche e le procedure aziendali (REG 01_REGOLAMENTO SULLE MODALITÀ DI UTILIZZO RISORSE ICT). I dipendenti e i collaboratori sono consapevoli delle minacce e istruiti sul corretto utilizzo dei sistemi informativi e dei dispositivi di proprietà (**attività di sensibilizzazione/formazione – Mod 710b - Programma annuale formazione)**. I dipendenti e i collaboratori sono consapevoli che le loro responsabilità e i loro doveri in materia di sicurezza delle informazioni rimangono validi anche dopo la cessazione o la modifica del rapporto di lavoro o di

Apio Srl
Sede legale: Via dei Teatini, 12 - 65127 Pescara (PE) – ITALIA
Sede operativa 1: Via Salara, 20 - 66020 San Giovanni Teatino (CH) - ITALIA
Contatti: +39 085 9396500 - info@apio.cc - www.apio.cc
P.IVA e C.F.: IT02094420680 – Capitale sociale: 14.881,58 €
Numero REA: PE - 153248 – PEC: apio@pec.it
Iscritta nell'apposita sezione speciale in qualità di PMI innovativa

collaborazione. I diritti di accesso attribuiti ai dipendenti e collaboratori in relazione alle informazioni aziendali, vengono rimossi al momento della cessazione del rapporto di lavoro o di collaborazione o aggiornati in seguito a cambiamenti intercorsi (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT).

4.1.9 Controlli sul personale

4.1.10 Sicurezza fisica

Le misure di controllo inerenti gli accessi fisici sono definite per assicurare che solo il personale autorizzato possa accedere alle aree aziendali. In particolare, le misure di sicurezza fisica vengono applicate dove sono conservati gli asset che contengono informazioni aziendali sensibili o critiche. Le misure di controllo inerenti gli accessi fisici sono regolarmente monitorate per garantire la loro efficacia nella protezione contro gli accessi non autorizzati. (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT).

4.1.11 Sicurezza ambientale

Le attrezzature sono protette anche dalle minacce ambientali (ad esempio incendio, inondazione, interferenze elettriche, ecc.). Gli ambienti di lavoro rispettano le politiche di APIO Srl in materia di salute e sicurezza. (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT)

4.1.12 Sicurezza tecnologici

4.1.13 Sicurezza delle operazioni

La sicurezza dell'infrastruttura tecnologica viene svolta grazie a controlli costanti da parte di fornitori di terze parti e con l'ausilio di sistemi di protezione (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT), al fine di mantenere la disponibilità dei dati in linea con i rischi associati. Inoltre, software e strutture di elaborazione delle informazioni sono protetti da codici malevoli/virus per garantire l'integrità del software e delle informazioni. I **log relativi agli eventi relativi alla sicurezza delle informazioni sono prodotti, conservati e rivisti regolarmente** (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT). Le attività di registrazione sono eseguite in conformità alla legislazione vigente. Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati sono ottenute in modo tempestivo, l'esposizione a tali vulnerabilità è oggetto di valutazione e vengono adottate misure appropriate per affrontare il rischio associato (REG 01_Regolamento sulle modalità di Utilizzo Risorse ICT).

Apio Srl
Sede legale: Via dei Teatini, 12 - 65127 Pescara (PE) – ITALIA
Sede operativa 1: Via Salara, 20 - 66020 San Giovanni Teatino (CH) - ITALIA
Contatti: +39 085 9396500 - info@apio.cc - www.apio.cc
P.IVA e C.F.: IT02094420680 – Capitale sociale: 14.881,58 €
Numero REA: PE - 153248 – PEC: apio@pec.it
Iscritta nell'apposita sezione speciale in qualità di PMI innovativa

4.1.14 Sicurezza delle comunicazioni

I dispositivi di comunicazione e di rete sono protetti per garantire l'integrità, la riservatezza e la disponibilità dei dati. La sicurezza dei dispositivi di rete è configurata correttamente, per assicurare la corretta segregazione tra i diversi ambienti di utilizzo. La sicurezza relativa allo scambio di dati è affrontata anche per mezzo di misure di sicurezza come l'utilizzo della crittografia dei dati.

4.1.15 Gestione degli incidenti relativi alla sicurezza delle informazioni

Gli eventi di sicurezza e le vulnerabilità associate ai sistemi informativi sono comunicate tempestivamente per intraprendere le appropriate azioni correttive (All_10 PCO_Piano di Continuità Operativa e Disaster Recovery). Sono messe in atto procedure di segnalazione degli eventi (All_10 PCO_Piano di Continuità Operativa e Disaster Recovery). In caso di violazione di dati personali, le attività di gestione sono conformi ai requisiti normativi vigenti (es. GDPR).

4.1.16 Gestione della Business Continuity e Disaster Recovery

Un sistema di gestione della Business Continuity è un insieme di processi, procedure e sistemi tecnologici finalizzati a garantire la continuità delle attività aziendali, in caso di eventi/disastri significativi, minimizzando i relativi impatti (es. perdita di ricavi, perdita di efficienza operativa, perdita di immagine e reputazione, ecc.). Per definire il sistema di gestione della Business Continuity è stato analizzato il contesto di business aziendale, definite le relative strategie di continuità operativa (All_10 PCO_Piano di Continuità Operativa e Disaster Recovery) e le misure tecnologiche ed organizzative per ripristinare sistemi, dati ed infrastrutture dopo il verificarsi di un evento che interrompa i processi aziendali (All_10 PCO_Piano di Continuità Operativa e Disaster Recovery). Il piano di Business Continuity e il piano di Disaster Recovery vengono se necessario testati, al fine di verificarne l'efficacia e l'efficienza e rivisti e aggiornati periodicamente in caso di cambiamenti significativi del contesto aziendale.

5 Impegno della direzione

APIO Srl si impegna quindi a:

- Comprendere le necessità degli utenti e pianificare le proprie attività per soddisfarle appieno;
- Operare nel rispetto delle richieste e dei requisiti del mercato di riferimento, delle leggi e regolamenti e di tutte le parti coinvolte nei propri processi:
- Identificare, controllare e migliorare costantemente le attività e gli obiettivi da perseguire, analizzando i risultati attesi;
- rendere disponibili tutte le risorse necessarie e assicurarsi che gli obiettivi pianificati siano compatibili con il contesto e gli indirizzi strategici dell'organizzazione;
- Comunicare l'importanza del proprio Sistema di Gestione e coinvolgere attivamente tutte le parti interessate, coordinandole e sostenendole;

Apio Srl
Sede legale: Via dei Teatini, 12 - 65127 Pescara (PE) – ITALIA
Sede operativa 1: Via Salara, 20 - 66020 San Giovanni Teatino (CH) - ITALIA
Contatti: +39 085 9396500 - info@apio.cc - www.apio.cc
P.IVA e C.F.: IT02094420680 – Capitale sociale: 14.881,58 €
Numero REA: PE - 153248 – PEC: apio@pec.it
Iscritta nell'apposita sezione speciale in qualità di PMI innovativa

- Valutare, trattare e gestire tutti i rischi associati ai processi aziendali con l'impegno ad eliminare anche i pericoli e ridurre i rischi per la salute e sicurezza sul lavoro e i rischi associati alla sicurezza delle informazioni al fine di adottare misure che consentano la mitigazione dei rischi e la preservazione dell'integrità, disponibilità e riservatezza delle informazioni
- Sfruttare e rinforzare le opportunità identificate;
- Coinvolgere il personale e tutti gli stakeholders nelle scelte operanti i risultati della qualità e nella consultazione riguardo la sicurezza nei luoghi di lavoro;
- Migliorare le prestazioni del proprio SGSI anche attraverso il riesame della Direzione;
- Rafforzare e consolidare le conoscenze e competenze del proprio personale, promuovendo la formazione costante e il perfezionamento delle capacità professionali;
- favorire l'identificazione dei collaboratori dell'azienda e la condivisione degli obiettivi aziendali, favorendo la consapevolezza del ruolo di ciascuno all'interno dell'azienda e la responsabilizzazione individuale;
- gestire le violazioni della sicurezza delle informazioni;
- sviluppare ed estendere efficaci ed efficienti processi di informazione e comunicazione, promuovendo il dialogo con tutte le parti interessate, per assicurare chiarezza e trasparenza nei rapporti, sia all'interno che all'esterno dell'organizzazione.

La Direzione si impegna a rendere operativa e mantenere attiva la presente Politica, comunicandola a tutto il personale e alle parti interessate che ne facciano richiesta; la sua adeguatezza è valutata periodicamente in occasione del Riesame della Direzione

Il Direttore Generale

