					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P34S					Titolo del documento: **Politica sui dispositivi mobili e Bring Your Own Device (BYOD)**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.1, 5.2, 6.1, 6.2, 8	Requisiti generali del SGSI e controlli relativi a dispositivi mobili/BYOD
ISO/IEC 27002:2022	Controlli 5.10–5.13	Controlli dettagliati per dispositivi mobili/BYOD e accesso remoto
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Controlli federali relativi a dispositivi, supporti e configurazioni
GDPR UE	Articolo 5(1)(f)	Protezione dei dati personali sugli endpoint mobili
NIS2 UE	Articolo 21(2)(d)	Protezione dei dispositivi critici per l'operatività, incluso il BYOD
DORA UE	Articoli 9, 10	Rischio ICT e continuità operativa per gli endpoint mobili
COBIT 2019	APO13, DSS01, DSS05	Governance IT, operazioni IT e controlli sui servizi di sicurezza

1. Finalità

1.1. La presente politica definisce i requisiti di sicurezza obbligatori per l'utilizzo dei dispositivi mobili, inclusi smartphone, tablet e laptop, per accedere a informazioni, sistemi o servizi aziendali.

1.2. Disciplina inoltre l'uso del Bring Your Own Device (BYOD) al fine di garantire la protezione dei dati dei clienti e dei dati aziendali, indipendentemente dalla proprietà del dispositivo.

1.3. La politica stabilisce misure di protezione coerenti per l'accesso mobile, contribuisce al conseguimento degli obiettivi di certificazione ISO/IEC 27001 e previene la perdita di dati o la compromissione derivante da endpoint mobili smarriti, rubati o utilizzati impropriamente.

1.4. Garantisce che l'utilizzo dei dispositivi mobili nelle piccole e medie imprese (PMI) prive di un team IT dedicato sia soggetto a misure di sicurezza sia tecniche sia procedurali, inclusi gli ambienti di lavoro da remoto e i servizi basati su cloud.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti i dipendenti, collaboratori esterni, tirocinanti e fornitori di servizi che:

2.1.1. utilizzano un dispositivo mobile per accedere a dati o sistemi aziendali, trattarli o memorizzarli

2.1.2. si collegano a servizi aziendali, inclusi posta elettronica, cartelle condivise, applicazioni cloud o sistemi interni tramite VPN

2.2. La politica si applica a:

2.2.1. tutti i dispositivi mobili: smartphone, tablet, laptop, aziendali o personali (BYOD)

2.2.2. tutti i sistemi operativi, ad es. iOS, Android, Windows, macOS

2.2.3. tutte le sedi e i contesti di utilizzo, inclusi ufficio, abitazione, lavoro da remoto e spazi pubblici

2.3. La politica si applica in tutti gli ambienti di lavoro e deve essere osservata indipendentemente dalla proprietà del dispositivo.

3. Obiettivi

3.1. Prevenire la perdita di dati: garantire che l'uso dei dispositivi mobili non esponga dati aziendali o dati sensibili dei clienti ad accessi non autorizzati, furto o uso improprio.

3.2. Definire regole chiare per il BYOD: stabilire condizioni applicabili per l'uso di dispositivi personali per finalità lavorative, assicurando misure di sicurezza giuridiche e tecniche.

3.3. Supportare la conformità normativa: soddisfare i requisiti previsti da ISO/IEC 27001, GDPR, NIS2 e altri obblighi di legge mediante pratiche di sicurezza mobile applicabili.

3.4. Ridurre al minimo il rischio operativo: diminuire la probabilità di interruzioni operative causate da uso improprio, compromissione o guasto dei dispositivi mobili.

3.5. Mantenere la fiducia dei clienti: dimostrare a clienti e partner che i loro dati rimangono protetti anche quando sono accessibili tramite dispositivi mobili o personali.

4. Ruoli e responsabilità

4.1. Direttore generale (GM):

4.1.1. mantiene la responsabilità complessiva della presente politica.

4.1.2. approva ogni utilizzo di accessi mobili e BYOD ai sistemi aziendali.

4.1.3. garantisce che gli accordi BYOD siano sottoscritti, archiviati e monitorati.

4.1.4. verifica che i fornitori esterni di servizi IT applichino le misure di protezione richieste per i dispositivi mobili.

4.2. Personale designato o supporto IT:

4.2.1. supporta la configurazione iniziale, la registrazione e l'impostazione dei dispositivi mobili utilizzati per lavoro.

4.2.2. applica i controlli di accesso relativi ai dispositivi mobili, le restrizioni sulle applicazioni e le politiche di monitoraggio.

4.2.3. supporta la risposta agli incidenti relativi ai dispositivi mobili, inclusi dispositivi smarriti, rubati o compromessi.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1. Riesame annuale

9.1.1. Il Direttore generale (GM) deve riesaminare la presente politica almeno una volta ogni 12 mesi.

9.1.2. Il riesame deve verificare il continuo allineamento con i requisiti della ISO/IEC 27001, con l'evoluzione delle tecnologie mobili e con i cambiamenti nelle operazioni aziendali.

9.1.3. Gli aggiornamenti devono inoltre tenere conto di incidenti recenti, risultati di audit o sviluppi normativi, ad es. GDPR, NIS2 e DORA.

9.2. Eventi attivatori per riesami intermedi

9.2.1. La presente politica deve essere aggiornata immediatamente se si verifica uno dei seguenti eventi:

9.2.1.1. incidente di sicurezza mobile rilevante, ad es. una violazione causata da un dispositivo smarrito o compromesso

9.2.1.2. modifica delle piattaforme supportate o degli strumenti di gestione dei dispositivi mobili

9.2.1.3. modifica legislativa o regolamentare che incide sull'uso dei dispositivi personali o sulla protezione dei dati

9.2.1.4. introduzione di nuove applicazioni, servizi o strumenti di terze parti utilizzati sui dispositivi mobili

9.3. Documentazione delle modifiche

9.3.1. Tutti i riesami e gli aggiornamenti devono essere documentati, inclusi la data del riesame, le modifiche apportate e l'approvazione del GM.

9.3.2. Deve essere conservata una cronologia del controllo delle versioni ai fini di audit.

9.4. Comunicazione e accesso

9.4.1. Il GM deve garantire che tutti gli utenti, inclusi dipendenti, collaboratori esterni e terze parti, siano informati delle modifiche.

9.4.2. Le versioni aggiornate devono essere rese facilmente accessibili, ad esempio nelle cartelle condivise o sulle piattaforme interne.

10. Politiche correlate e collegamenti

10.1. La presente politica fa parte del corpus complessivo delle politiche SME per la sicurezza delle informazioni e deve essere applicata congiuntamente alle seguenti:

10.1.1. P4S – Politica di controllo degli accessi: definisce i requisiti per la gestione dell'accesso sicuro ai sistemi, inclusi quelli accessibili tramite dispositivi mobili. Impone requisiti di igiene delle password e controlli di sessione.

10.1.2. P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: garantisce che gli utenti siano formati sull'uso sicuro dei dispositivi mobili, sulla segnalazione degli incidenti e sulle condizioni del BYOD.

10.1.3. P17S – Politica di protezione dei dati e privacy: stabilisce il trattamento conforme al GDPR dei dati personali e dei dati aziendali sulle piattaforme mobili, soprattutto quando per lavoro sono utilizzati dispositivi personali.

10.1.4. P9S – Politica di lavoro da remoto: è allineata alle regole di utilizzo dei dispositivi mobili durante il lavoro fuori sede o da casa, incluse la gestione dei dispositivi e le misure di protezione per l'accesso alla rete.

10.1.5. P30S – Politica di risposta agli incidenti: fornisce il quadro di riferimento per la risposta agli incidenti relativi ai dispositivi mobili, inclusi i dispositivi compromessi o smarriti.

10.2. Tali politiche correlate operano congiuntamente per costituire un insieme completo di controlli per la sicurezza dei dispositivi mobili nelle PMI prive di personale IT dedicato, garantendo applicabilità, trasparenza e preparazione alla certificazione.

11. Norme e quadri di riferimento

11.1. La presente politica supporta il pieno allineamento con i seguenti standard di sicurezza e conformità:

11.2. ISO/IEC 27001:

11.2.1. Clausola 5.1 – Leadership e impegno: garantisce supervisione della direzione e responsabilità per l'accesso mobile e il BYOD

11.2.2. Clausola 6.1 – Azioni per affrontare rischi e opportunità: richiede che i rischi di sicurezza mobile siano valutati e trattati

11.2.3. Clausola 8.1 – Pianificazione e controllo operativi: richiede procedure coerenti per l'accesso mobile al fine di proteggere i dati aziendali

11.3. ISO/IEC 27002:

11.3.1. Controlli 5.10 (Uso dei dispositivi mobili), 5.11 (Telelavoro), 5.12 (Accesso remoto) e 5.13 (BYOD): forniscono linee guida applicative per la gestione dei rischi dei dispositivi nel contesto di una piccola impresa

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Controllo degli accessi per dispositivi mobili: richiede impostazioni di sicurezza per l'uso autorizzato dei dispositivi mobili

11.4.2. AC-20 – Uso di sistemi esterni: disciplina i rischi connessi al BYOD e all'accesso remoto

11.4.3. CM-6 – Impostazioni di configurazione: impone impostazioni sicure predefinite e personalizzate sulle piattaforme mobili

11.4.4. MP-7 – Uso dei supporti: disciplina l'uso corretto e le restrizioni relative all'archiviazione mobile e all'accesso ai dati

11.5. GDPR UE (2016/679):

11.5.1. Articolo 5(1)(f) – Integrità e riservatezza: richiede la protezione dei dati mediante adeguate misure di sicurezza dei dati personali, in particolare sulle piattaforme mobili

11.5.2. Articolo 32 – Sicurezza del trattamento: impone l'adozione di misure tecniche e organizzative (TOM) adeguate per proteggere i dati accessibili o memorizzati sui dispositivi mobili

11.6. Direttiva UE NIS2 (2022/2555):

11.6.1. Articolo 21(2)(d) – Misure di sicurezza dei dispositivi: richiede controlli di sicurezza per hardware e software utilizzati per accedere a sistemi critici per l'operatività, inclusi i dispositivi personali

11.7. DORA UE (2022/2554):

11.7.1. Articolo 9 – Quadro di riferimento per la gestione del rischio ICT: richiede la protezione degli endpoint mobili utilizzati per comunicazioni aziendali critiche e servizi cloud

11.7.2. Articolo 10 – Continuità operativa ICT: impone il mantenimento di un accesso sicuro ai sistemi aziendali anche durante interruzioni o lavoro da remoto

11.8. COBIT 2019:

11.8.1. APO13 – Gestire la sicurezza: richiede all'organizzazione di applicare politiche per dispositivi mobili e BYOD allineate al rischio aziendale

11.8.2. DSS01 – Gestire le operazioni: garantisce l'applicazione tecnica dei meccanismi di accesso sicuro

11.8.3. DSS05 – Gestire i servizi di sicurezza: disciplina il coinvolgimento di terze parti nel mantenimento di ambienti mobili sicuri e nel coordinamento della risposta agli incidenti