					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P34					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 standard e normative

Standard/Normativa	Clausola/Articolo	Commento
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Applica controlli di sicurezza e requisiti di conformità
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Fornisce controlli dettagliati per la gestione dei dispositivi mobili
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Controllo degli accessi, accesso remoto, configurazione e requisiti di sicurezza per i dispositivi mobili
GDPR UE	5(1)(f), 25, 32	Requisiti obbligatori in materia di privacy, cifratura dei dati e sicurezza del trattamento
NIS2 UE	21(2)(d)	Misure tecniche e organizzative di protezione per l'accesso mobile
DORA UE	9, 10	Gestione del rischio ICT e requisiti di sicurezza per i dispositivi mobili
COBIT 2019	APO13.02, DSS01.04, BAI09	Piani per la sicurezza delle informazioni, configurazione degli asset e controlli per ambienti mobili

1. Finalità

1.1 La presente politica stabilisce i requisiti di sicurezza, conformità e operativi per l'utilizzo dei dispositivi mobili e delle tecnologie personali (BYOD – Bring Your Own Device) nell'accesso ai sistemi, alle applicazioni e ai dati dell'organizzazione.

1.2 La politica mira a garantire la riservatezza, l'integrità e la disponibilità (CIA) delle informazioni aziendali a cui si accede o che vengono trattate tramite endpoint mobili, inclusi smartphone, tablet, laptop e dispositivi ibridi.

1.3 La politica stabilisce inoltre i controlli tecnici e procedurali necessari a mitigare rischi quali perdita di dati, accesso non autorizzato, smarrimento o furto del dispositivo e compromissione delle applicazioni mobili.

1.4 La presente politica supporta la conformità normativa e contrattuale, consentendo al contempo una produttività mobile sicura per dipendenti, collaboratori esterni e terze parti autorizzate.

2. Ambito di applicazione

2.1 La presente politica si applica a tutto il personale, inclusi dipendenti, collaboratori esterni, tirocinanti e fornitori terzi di servizi, che utilizzano dispositivi mobili per accedere a dati, sistemi, applicazioni o piattaforme di comunicazione aziendali.

2.2 Essa si applica a tutti i dispositivi di mobile computing, inclusi, a titolo esemplificativo e non esaustivo:

2.2.1 Smartphone e tablet (iOS, Android, ecc.)

2.2.2 Laptop e ultrabook (Windows, macOS, Linux)

2.2.3 Dispositivi indossabili e dispositivi intelligenti ibridi in grado di sincronizzare dati

2.3 Si applica indipendentemente dal fatto che il dispositivo sia di proprietà aziendale o personale nell'ambito di un accordo BYOD.

2.4 La politica comprende tutti i vettori di accesso, incluse VPN, infrastruttura desktop virtuale (VDI), applicazioni cloud, posta elettronica, piattaforme di collaborazione (ad es. SharePoint, Teams) e strumenti di sincronizzazione dei file (ad es. OneDrive, Dropbox se autorizzato).

2.5 Include l'utilizzo in contesti di lavoro da remoto, in sede, in viaggio o in modalità di lavoro ibrida.

3. Obiettivi

3.1 Ridurre il rischio di compromissione, perdita o divulgazione dei dati derivante da un utilizzo non sicuro dei dispositivi mobili.

3.2 Applicare controlli di sicurezza coerenti e verificabili su tutti gli endpoint mobili, indipendentemente dal modello di proprietà (aziendale o BYOD).

3.3 Garantire che l'utilizzo dei dispositivi mobili sia conforme alla ISO/IEC 27001 e agli altri quadri normativi applicabili in materia di privacy, protezione dei dati e cybersicurezza.

3.4 Favorire l'integrazione sicura dei dispositivi mobili nei processi operativi, di comunicazione e di collaborazione dell'organizzazione.

3.5 Definire in modo chiaro responsabilità e processi per la gestione dei dispositivi mobili (MDM), inclusi registrazione, cancellazione remota, cifratura, autenticazione e monitoraggio.

3.6 Tutelare i diritti alla privacy delle persone che utilizzano i propri dispositivi, salvaguardando al contempo le informazioni sensibili dell'organizzazione.

4. Ruoli e responsabilità

4.1 Responsabile della Sicurezza delle Informazioni (CISO) / Responsabile della Sicurezza IT

4.1.1 Definisce la politica e gli standard tecnici per l'utilizzo dei dispositivi mobili e del BYOD.

4.1.2 Supervisiona la conformità, la risposta agli incidenti e la gestione delle eccezioni relative ai controlli sui dispositivi mobili.

4.1.3 Si coordina con le funzioni Legale e Compliance e con le Risorse Umane (HR) per garantire che l'applicazione della politica sia giuridicamente fondata e allineata al contesto organizzativo.

4.2 Amministratore IT / Amministratore MDM

4.2.1 Gestisce il provisioning degli accessi, la registrazione e la configurazione dei dispositivi mobili tramite soluzioni MDM.

4.2.2 Applica controlli a livello di dispositivo (ad es. cifratura, PIN, controlli sulle applicazioni).

4.2.3 Esegue la cancellazione remota, il blocco del dispositivo e la revoca degli accessi quando necessario.

[... 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 La presente politica deve essere riesaminata almeno annualmente dal Responsabile della Sicurezza delle Informazioni (CISO) o da un Responsabile della Sicurezza delle Informazioni designato, per garantire l'allineamento con:

9.1.1 Modifiche alle piattaforme dei sistemi operativi mobili, alle tecnologie MDM o agli standard di autenticazione

9.1.2 Modifiche normative o contrattuali che incidono sulla protezione dei dati mobili (ad es. GDPR, DORA, NIS2)

9.1.3 Revisioni dei set di controlli ISO/IEC 27001:2022, ISO/IEC 27002:2022 o NIST SP 800-53 Rev.5

9.1.4 Feedback da audit, analisi post-incidente o segnalazioni dei dipendenti

9.2 Riesami intermedi possono essere attivati da:

9.2.1 Incidenti di sicurezza che coinvolgono dispositivi mobili o piattaforme BYOD

9.2.2 Notifiche del fornitore relative a vulnerabilità ad alto rischio nelle piattaforme supportate

9.2.3 Introduzione di nuove applicazioni mobili o piattaforme di collaborazione utilizzate per le operazioni aziendali

9.3 Gli aggiornamenti della politica devono essere:

9.3.1 Documentati nella cronologia delle versioni della politica

9.3.2 Comunicati a tutto il personale e ai collaboratori esterni interessati

9.3.3 Confermati nuovamente con presa d'atto aggiornata da parte di tutti gli utenti BYOD

9.4 Tutti i riesami e le revisioni devono essere formalmente approvati dalla Direzione esecutiva e registrati nel Registro delle modifiche alle politiche.

10. Politiche correlate e collegamenti

10.1 La presente politica è interdipendente con diverse politiche chiave del framework SGSI dell'organizzazione. I principali collegamenti includono:

10.1.1 P1 – Politica per la sicurezza delle informazioni: stabilisce i principi generali di governance per tutti i controlli di sicurezza delle informazioni, inclusi quelli relativi all'utilizzo dei dispositivi mobili.

10.1.2 P3 – Politica di uso accettabile: definisce i comportamenti consentiti e le restrizioni relative all'uso della tecnologia, applicabili direttamente anche all'accesso mobile e BYOD.

10.1.3 P9 – Politica di lavoro da remoto: definisce ulteriori obblighi di sicurezza per gli ambienti di lavoro mobili, integrando i controlli specifici sui dispositivi mobili previsti dalla presente politica.

10.1.4 P13 – Politica di classificazione ed etichettatura dei dati: disciplina le modalità di gestione dei dati sui dispositivi mobili in base al livello di classificazione, con impatto su archiviazione, trasferimento e applicazione della cifratura.

10.1.5 P22 – Politica di registrazione e monitoraggio: supporta la raccolta e il riesame dei log di accesso mobile per rilevare anomalie o violazioni.

10.1.6 P30 – Politica di risposta agli incidenti (P30): disciplina le modalità di trattamento ed escalation degli incidenti relativi ai dispositivi mobili (ad es. smarrimento del dispositivo, accesso non autorizzato).

10.1.7 P33 – Politica di monitoraggio dell'audit e della conformità: fornisce la base per controlli periodici sulla conformità della sicurezza mobile, incluso il rispetto della politica BYOD.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata ai quadri di riferimento internazionalmente riconosciuti in materia di cybersicurezza e agli obblighi giuridici applicabili, al fine di garantire l'utilizzo sicuro dei dispositivi mobili e delle tecnologie personali (BYOD) in contesti aziendali.

11.2 ISO/IEC 27001:

11.2.1 Clausola 5.10 – Uso accettabile delle informazioni e degli asset: richiede controlli per l'utilizzo responsabile degli asset aziendali, inclusi i dispositivi mobili.

11.2.2 Clausola 5.11 – Lavoro da remoto: disciplina le pratiche sicure per l'accesso ai sistemi dall'esterno dei locali aziendali.

11.2.3 Clausola 5.12 – Uso dei dispositivi mobili: richiede controlli basati sul rischio per gli endpoint mobili e le configurazioni BYOD.

11.2.4 Clausola 5.13 – Trasferimento delle informazioni: impone la protezione delle informazioni trasferite tramite canali mobili.

11.3 ISO/IEC 27002:2022 – Controlli da 5.10 a 5.13:

11.3.1 I controlli dell'Allegato A da 5.10 a 5.13 specificano come devono essere applicati all'interno di un SGSI l'accesso mobile, la cifratura, il monitoraggio e la mitigazione della perdita. Tali controlli forniscono indicazioni di dettaglio per proteggere gli endpoint mobili, applicare la containerizzazione, monitorare l'integrità del dispositivo e garantire configurazioni BYOD rispettose della privacy.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Controllo degli accessi per i dispositivi mobili: definisce le protezioni di base, incluse cifratura, autenticazione e applicazione dell'MDM.

11.4.2 AC-17 – Accesso remoto: richiede autenticazione sicura e protezioni di sessione per gli utenti mobili remoti.

11.4.3 CM-7 – Principio di minima funzionalità: supporta la rimozione di applicazioni e funzionalità non necessarie dagli endpoint mobili per ridurre il rischio.

11.4.4 MP-5 – Protezione del trasporto dei supporti: disciplina la trasmissione sicura dei dati dai sistemi mobili verso destinazioni esterne o cloud.

11.4.5 SC-12 – Definizione delle chiavi crittografiche: impone l'utilizzo di protocolli crittografici sicuri per la comunicazione e l'archiviazione mobile.

11.5 GDPR UE (2016/679):

11.5.1 Articolo 5(1)(f) – Integrità e riservatezza: richiede alle organizzazioni di proteggere i dati personali sui dispositivi mobili contro accessi non autorizzati o illeciti.

11.5.2 Articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita: richiede che la tutela della privacy sia integrata nei processi BYOD e MDM.

11.5.3 Articolo 32 – Sicurezza del trattamento: impone controlli basati sul rischio (ad es. cifratura, autenticazione, controllo degli accessi) per i dati personali sulle piattaforme mobili.

11.6 Direttiva UE NIS2 (2022/2555):

11.6.1 Articolo 21(2)(d): richiede che l'accesso mobile a sistemi e informazioni critici sia protetto mediante adeguate misure tecniche e organizzative, quali controllo degli endpoint, cifratura e monitoraggio.

11.7 DORA UE (2022/2554):

11.7.1 Articolo 9 – Quadro di gestione del rischio ICT: richiede che i soggetti del settore finanziario mitighino i rischi connessi all'accesso mobile e remoto nell'ambito della resilienza operativa.

11.7.2 Articolo 10 – Requisiti di sicurezza dei sistemi ICT: richiede architetture mobili sicure, monitoraggio e meccanismi di risposta alle minacce informatiche originate da dispositivi mobili.

11.8 COBIT 2019:

11.8.1 APO13.02 – Definire e mantenere un piano per la sicurezza delle informazioni: richiede che l'utilizzo dei dispositivi mobili, incluso il BYOD, sia integrato nelle strategie di sicurezza dell'organizzazione.

11.8.2 DSS01.04 – Gestire configurazione e integrità degli asset: si applica al controllo della configurazione e al deployment sicuro dei dispositivi mobili.

11.8.3 BAI09.01 – Definire e mantenere i controlli: supporta l'implementazione di misure di sicurezza tecniche e procedurali per operazioni mobili e da remoto sicure.