					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P38					Titolo del documento: **Politica per le comunicazioni sicure e l'autenticazione a più fattori**							
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**

Allineata a standard e regolamenti

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
GDPR UE	Art. 32(1)(b)	
NIS2 UE	Art. 21(2)(j)	
DORA UE	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Finalità

1.1 Definire i requisiti per l'uso di soluzioni di autenticazione a più fattori (MFA) o di autenticazione continua per l'accesso ai sistemi, in conformità all'articolo 21(2)(j) della NIS2.

1.2 Stabilire controlli per comunicazioni vocali, video, testuali e di emergenza sicure, al fine di tutelare la riservatezza e l'integrità delle informazioni.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i meccanismi di autenticazione e ai sistemi di comunicazione (chiamate vocali, videoconferenze, messaggistica e sistemi di notifica di emergenza) utilizzati dall'organizzazione.

2.2 Si applica a tutti i dipendenti e ai collaboratori esterni, nonché a tutte le parti esterne che utilizzano i canali di comunicazione dell'organizzazione o accedono ai relativi sistemi informativi e di rete.

3. Obiettivi

3.1 Garantire che solo gli utenti adeguatamente autenticati ottengano accesso ai sistemi, riducendo il rischio di accessi non autorizzati mediante l'implementazione dell'autenticazione a più fattori (MFA).

3.2 Garantire che le comunicazioni interne e di emergenza siano trasmesse mediante modalità sicure (ad esempio canali cifrati), prevenendo intercettazioni o manomissioni.

3.3 Soddisfare i requisiti della NIS2 in materia di autenticazione forte e comunicazioni sicure, rafforzando la resilienza informatica complessiva.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO) / Sicurezza IT: definisce e mantiene i meccanismi MFA e gli strumenti di comunicazione sicura; assicura l'applicazione tecnica della presente politica.

4.2 Amministratori IT: implementano l'MFA per i sistemi pertinenti e configurano le piattaforme di comunicazione sicura approvate; monitorano la conformità.

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

9. Monitoraggio e audit

9.1 La Sicurezza IT deve monitorare con continuità i log di autenticazione per individuare eventuali tentativi di accesso con un solo fattore o anomalie nei fallimenti MFA. I log dei sistemi di comunicazione

sicura, ove applicabili, devono essere monitorati per rilevare tentativi di accesso non autorizzato o modifiche della configurazione.

9.2 La funzione di audit interno / conformità deve riesaminare annualmente il rispetto dei requisiti di implementazione dell'MFA, verificando che tutti i sistemi critici ne impongano l'uso, e accertare che per le comunicazioni sensibili siano utilizzati esclusivamente canali sicuri approvati. Le risultanze devono essere comunicate alla direzione con le relative raccomandazioni.

10. Riesame e manutenzione

10.1 La presente politica deve essere sottoposta a riesame almeno annuale e in occasione di qualsiasi grave incidente di sicurezza o di nuovi rischi identificati relativi all'autenticazione o alle comunicazioni (ad esempio nuovi vettori di minaccia contro l'MFA o rilevazione dell'uso di comunicazioni non sicure).

10.2 Le revisioni devono essere apportate secondo necessità per affrontare l'evoluzione delle tecnologie (ad esempio adozione di soluzioni di autenticazione continua più robuste) o per conformarsi a indicazioni normative aggiornate (quali future raccomandazioni ENISA sulle comunicazioni sicure).

11. Politiche correlate e collegamenti

11.1 P01 – Politica per la sicurezza delle informazioni. Stabilisce le misure di sicurezza per autenticazione e comunicazioni a livello aziendale.

11.2 P04 – Politica di controllo degli accessi. Definisce la governance degli accessi che l'MFA prevista dalla P38 rende operativa.

11.3 P11 – Politica di gestione degli account utente e dei privilegi. Collega l'MFA al ciclo di vita degli accessi privilegiati.

11.4 P18 – Politica sui controlli crittografici. Definisce i meccanismi approvati di crittografia e gestione delle chiavi per le comunicazioni sicure.

11.5 P21 – Politica di sicurezza della rete. Protegge i canali di trasporto utilizzati da voce, video e messaggistica.

11.6 P22 – Politica di registrazione e monitoraggio. Disciplina il monitoraggio degli eventi di autenticazione e dell'uso dei canali sicuri.

11.7 P32 – Politica di continuità operativa e ripristino in caso di disastro. Protegge le comunicazioni di emergenza durante le crisi.

11.8 P08 – Politica di consapevolezza e formazione sulla sicurezza delle informazioni. Forma gli utenti su MFA e corretto utilizzo dei canali.

12. Riferimenti

12.1 Direttiva NIS2 (UE 2022/2555), articolo 21(2), lettera (j) (uso dell'autenticazione a più fattori e di comunicazioni protette)

12.2 Regolamento di esecuzione della Commissione (UE) 2024/2690, Allegato, sezione 11 (requisiti di controllo degli accessi, inclusa l'MFA per gli account privilegiati)

12.3 ISO/IEC 27001:2022 e ISO/IEC 27002:2022