

Documento	CHECK LIST PRIVACY 4.0 + ISO27001 + CSF/NIST
Adempimenti	VERIFICA VR-DPIA E AUDIT PERIODICO SISTEMA
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, RDTA, DVR/IP
Basi giuridiche	Modulo lista di controlli Sistema TQM integrato

Procedura operativa di risposta agli incidenti informatici

La Sicurezza Informatica aziendale è condotta a diversi livelli di implementazione

AUDIT ICT (*SISTEMA TQM integrazione ISO-27001/ISO-20000*)

1. [HARDWARE: check list di controllo e/o configurazioni](#)
2. [SOFTWARE: check list di controllo e/o configurazioni](#)
3. [NETWORK: check list di controllo e/o configurazioni](#)
4. [AUTOMAZIONE: check list di controllo e/o configurazioni](#)
5. [FATTORI UMANI: check list di controllo e/o configurazioni](#)

1. [HARDWARE: check list di controllo e/o configurazioni](#)

Controlli sugli Apparati
Badge di identificazione
Privilegi per l'accesso fisico
Protezione fisica dei dispositivi
Data Centers
Controlli ambientali
Cavi e armadi di cablaggio
Utilizzo e distruzione di dispositivi elettronici
Stampe

2. [SOFTWARE: check list di controllo e/o configurazioni](#)

Applicazione e sistemi operativi
Assegnazione Privilegi
Utilizzo Applicazioni
Circolazione dati e modifiche
Sistemi di autenticazione
Policy di Autenticazione
Passwords
Autenticazione Avanzata
Biometria

3. [NETWORK: check list di controllo e/o configurazioni](#)

Connettività costante
Connessione di un apparato alla rete
Dispositivi non autorizzati
Gestione della rete
Monitoraggio di rete
Connettività Cloud e Piattaforme di condivisione
Connettività e mobilità
Laptop e smartphone
VPN e Modem
Cifatura
Sicurezza preventiva, firewall etc



4. AUTOMAZIONE: check list di controllo e/o configurazioni

Strategie di backup

Dispositivi periferici

Sensori remoti e sistemi di controllo

5. FATTORI UMANI: check list di controllo e/o configurazioni

Gestione degli incidenti (dipendenti / incaricati e soggetti autorizzati)

Amministrazione della sicurezza

Azioni amministrative

Audit e review esterne

Senior Management

Azioni individuali dei dipendenti

Attività di reporting da parte dei soggetti autorizzati

Monitoraggio delle attività dei dipendenti

Formazione dei dipendenti in materia di cyber security

Responsabilità personale in tema di sicurezza