Codice: SOA	
Titolo: Dichiarazione di Applicabilità	

Stato delle edizioni

Edizione n°	***Motivo della edizione***	**Data**
00	Prima emissione a fronte della norma UNI EN ISO 27001:2013	19/12/2019
01	Revisione effettuata a seguito del Risk Assessment	01/06/2020

Approvazione ed emissione

	Data	**Firma**
Redatto da: RSGSI	01/06/2020	RSGSI
Verificato da: DG		DG
Approvato da: DG		DG

Stato della copia

Tipo di copia: ☐ Copia controllata – copia elettronica	☐■ Copia non controllata – formato elettronico
Copia n°:	Copia n°: 01/01
Consegnata a:	Consegnata a:
In data:	In data:
Firma DG per distribuzione:	Firma DG per distribuzione:
Firma ricevimento:	Firma ricevimento:

In caso di consegna in formato elettronico del documento, non è presente la firma per la distribuzione e per il ricevimento.

Dichiarazione di applicabilità

Sez.	Controllo / Obiettivo di Controllo	Applicato (A) / Non applicato (NA)
5.1.1	Politiche per la sicurezza delle informazioni	A
5.1.2	Riesame delle Politiche per la sicurezza delle informazioni	A
6.1.1	Ruoli e responsabilità per la sicurezza delle informazioni	A
6.1.2	Separazione dei compiti (SoD)	A
6.1.3	Contatti con le autorità	A
6.1.4	Contatti con gruppi specialistici	A
6.1.5	Sicurezza delle informazioni nella gestione dei progetti	A
6.2.1	Politica per i dispositivi portatili	A
6.2.2	Telelavoro	A
7.1.1	Screening	A
7.1.2	Termini e condizioni d'impiego	A
7.2.1	Responsabilità della direzione	A
7.2.2	Consapevolezza, istruzione, formazione ed addestramento sulla sicurezza delle informazioni	A
7.2.3	Processo disciplinare	A
7.3.1	Cessazione o variazione delle responsabilità durante il rapporto di lavoro	A
8.1.1	Inventario degli asset	A
8.1.2	Responsabilità degli asset	A
8.1.3	Utilizzo accettabile degli asset	A
8.1.4	Restituzione degli asset	A
8.2.1	Classificazione delle informazioni	A
8.2.2	Etichettatura delle informazioni	A
8.2.3	Trattamento degli asset	A
8.3.1	Gestione dei supporti rimovibili	A
8.3.2	Dismissione dei supporti	A
8.3.3	Trasporto dei supporti fisici	A
9.1.1	Politica di controllo degli accessi	A
9.1.2	Accesso alle reti ed ai servizi di rete	A
9.2.1	Registrazione e deregistrazione degli utenti	A

9.2.2	Provisioning degli accessi degli utenti	A
9.2.3	Gestione dei diritti di accesso privilegiato	A
9.2.4	Gestione delle informazioni segrete di autenticazione degli utenti	A
9.2.5	Riesame dei diritti di accesso degli utenti	A
9.2.6	Rimozione o adattamento dei diritti di accesso	A
9.3.1	Utilizzo delle informazioni segrete di autenticazione	A
9.4.1	Limitazione dell'accesso alle informazioni	A
9.4.2	Procedure di log on sicure	A
9.4.3	Sistema di gestione delle password	A
9.4.4	Uso di programmi di utilità privilegiati	A
9.4.5	Controllo degli accessi al codice sorgente dei programmi	NA
10.1.1	Politica sull'uso dei controlli crittografici	NA
10.1.2	Gestione delle Chiavi	NA
11.1.1	Perimetro di sicurezza fisica	A
11.1.2	Controlli di acesso fisico	A
11.1.3	Rendere sicuri uffici, locali e strutture	A
11.1.4	Protezione contro minacce esterne ed ambientali	A
11.1.5	Lavoro in aree sicure	A
11.1.6	Aree di carico e scarico	A
11.2.1	apparecchiature e loro disposizione	A
11.2.2	Infrastrutture di supporto	A
11.2.3	Sicurezza dei cablaggi	A
11.2.4	Manutenzione delle apparecchiature	A
11.2.5	Trasferimento degli asset	A
11.2.6	Sicurezza delle apparecchiature e degli asset all'esterno delle sedi	A
11.2.7	Dismissione sicura o utilizzo delle apparecchiature	A
11.2.8	Apparecchiature incustodite degli utenti	A
11.2.9	Politica di schermo e scrivanie pulite	A
12.1.1	Procedure operative documentate	A
12.1.2	Gestione dei cambiamenti	A
12.1.3	Gestione delle capacità	A

12.1.4	Separazione degli ambienti di sviluppo, test e produzione	NA
12.2.1	Controlli contro il malware	A
12.3.1	Backup delle informazioni	A
12.4.1	Raccolta dei log degli eventi	A
12.4.2	Protezione delle informazioni di log	A
12.4.3	Log di amministratori e operatori	A
12.4.4	Sincronizzazione degli orologi	A
12.5.1	Installazione del software sui sistemi di produzione	A
12.6.1	Gestione delle vulnerabilità tecniche	A
12.6.2	Limitazioni all'installazione del software	A
12.7.1	Controlli per l'audit dei sistemi informativi	A
13.1.1	Controlli di rete	A
13.1.2	Sicurezza dei servizi di rete	A
13.1.3	Segregazione nelle reti	A
13.2.1	Politiche e procedure per il trasferimento delle informazioni	A
13.2.2	Accordi per il trasferimento delle informazioni	A
13.2.3	Messaggistica elettronica	A
13.2.4	Accordi di riservatezza o di non divulgazione (NDA)	A
14.1.1	Analisi e specifica dei requisiti per la sicurezza delle informazioni	NA
14.1.2	Sicurezza dei servizi applicativi su reti pubbliche	NA
14.1.3	Protezione delle transazioni dei servizi applicativi	NA
14.2.1	Politica per lo sviluppo sicuro	NA
14.2.2	Procedure per il controllo dei cambiamenti di sistema	NA
14.2.3	Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative	NA
14.2.4	Limitazione ai cambiamenti dei pacchetti software	NA
14.2.5	Principi per l'ingegnerizzazione sicura dei sistemi	NA
14.2.6	Ambiente di sviluppo sicuro	NA
14.2.7	Sviluppo affidato all'esterno	NA
14.2.8	Test di sicurezza dei sistemi	NA
14.2.9	Test di accettazione dei sistemi	NA
14.3.1	Protezione dei dati di test	NA

15.1.1	Politica per la sicurezza delle informazioni nei rapporti con i fornitori	A
15.1.2	Indirizzare la sicurezza all'interno degli accordi con i fornitori	A
15.1.3	Filiera di fornitura per l'ICT	A
15.2.1	Monitoraggio e riesame dei servizi dei fornitori	A
15.2.2	Gestione dei cambiamenti ai servizi dei fornitori	A
16.1.1	Responsabilità e procedure	A
16.1.2	Segnalazione degli eventi relativi alla sicurezza delle informazioni	A
16.1.3	Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni	A
16.1.4	Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	A
16.1.5	Risposta agli incidenti relativi alla sicurezza delle informazioni	A
16.1.6	Apprendimento dagli incidenti relativi alla siscurezza delle informazioni	A
16.1.7	Raccolta di evidenze	A
17.1.1	Pianificazione della continuità della sicurezza delle informazioni	A
17.1.2	Attuazione della continuità della sicurezza delle informazioni	A
17.1.3	Verifica, riesame e valutazione della continuità della sicurezza delle informazioni	A
17.2.1	Disponibilità delle strutture per l'elaborazione delle informazioni	A
18.1.1	Identificazione della legislazione applicabile a dei requisiti contrattuali	A
18.1.2	Diritti di proprietà intellettuale	A
18.1.3	Protezione delle registrazioni	A
18.1.4	Privacy e protezione dei dati personali	A
18.1.5	Regolamentazione sui controlli crittografici	A
18.2.1	Riesame indipendente della sicurezza delle informazioni	A
18.2.2	Conformità alle politiche ed alle norme per la sicurezza	A
18.2.3	Verifica tecnica della conformità	A

Esclusioni

Sez.	Controllo / Obiettivo di Controllo	Motivazione esclusione
9.4.5	Controllo degli accessi al codice sorgente dei programmi	La DG ed i dipendenti non hanno acccesso al codice sorgente
10.1.1	Politica sull'uso dei controlli crittografici	La crittografia non viene utilizzata direttamente dall'azienda
10.1.2	Gestione delle Chiavi	La crittografia non viene utilizzata direttamente dall'azienda
12.1.4	Separazione degli ambienti di sviluppo, test e produzione	Non viene eseguito sviluppo software
14.1.1	Analisi e specifica dei requisiti per la sicurezza delle informazioni	Non viene eseguito sviluppo software
14.1.2	Sicurezza dei servizi applicativi su reti pubbliche	Non vengono utilizzate reti pubbliche
14.1.3	Protezione delle transazioni dei servizi applicativi	Non vengono effettuate transazioni dei servizi applicativi
14.2.1	Politica per lo sviluppo sicuro	Non viene eseguito sviluppo software
14.2.2	Procedure per il controllo dei cambiamenti di sistema	Non viene eseguito sviluppo software
14.2.3	Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative	Non viene eseguito sviluppo software
14.2.4	Limitazione ai cambiamenti dei pacchetti software	Non viene eseguito sviluppo software
14.2.5	Principi per l'ingegnerizzazione sicura dei sistemi	Non viene eseguito sviluppo software
14.2.6	Ambiente di sviluppo sicuro	Non viene eseguito sviluppo software
14.2.7	Sviluppo affidato all'esterno	Non viene eseguito sviluppo software
14.2.8	Test di sicurezza dei sistemi	Non viene eseguito sviluppo software
14.2.9	Test di accettazione dei sistemi	Non viene eseguito sviluppo software
14.3.1	Protezione dei dati di test	Non viene eseguito sviluppo software

Documentazione e registri associati

Nome documento/registrazione	Proprietario
Matrice controlli (documento ad uso interno)	RSGSI

Gestione Documentale

Il presente documento è valido a partire dal 19/12/2019 ed aggiornato in data 01/06/2020

Il presente documento viene periodicamente e comunque con cadenza almeno semestrale al fine di garantire il rispetto dei seguenti criteri previsti.

- Conformità ai requisiti della norma ISO 27001:2013