



PIANO DI SICUREZZA E CONTINUITÀ

Stato	Redatto e aggiornato da	Rivisto e approvato da	Validato da Ufficio Certificazioni e Compliance
Approvato	Alex Bertoldi	Roberto Conci	SI
	22/04/2025	22/04/2025	22/04/2025

LISTA DI DISTRIBUZIONE

A tutti gli stakeholder

STORIA DELLE MODIFICHE APPORTATE

VERSIONE	DATA	PARAGRAFO	MODIFICHE
1.0	14/06/2024	-	Prima emissione
1.1	03/07/2024	3, 4 e 20	Riportata la tabella delle certificazioni con i relativi campi di applicazione Aggiunto il paragrafo relativo ai fornitori
1.2	22/04/2025	12.6, 12.7, 15, 15.1, 15.4	Aggiornamento dei paragrafi indicati

SOMMARIO

1. SCOPO	7
2. CAMPO DI APPLICAZIONE	7
3. NORMATIVA	7
4. CERTIFICAZIONI E POLITICHE	7
5. APPROCCIO ALLA SICUREZZA DELLE INFORMAZIONI	11
6. STRATEGIA AZIENDALE	11
6.1. IL CICLO DI VITA DELLA CYBERSECURITY	12
7. RUOLI E RESPONSABILITÀ	12
8. ANALISI DEI RISCHI	15
8.1. IDENTIFICAZIONE DEI RISCHI	15
8.1.1. IDENTIFICAZIONE DELLE MINACCE	15
8.1.2. VALUTAZIONE DEI RISCHI	15
8.2. VALUTAZIONE DELLE VULNERABILITÀ DEI SISTEMI	16
8.3. TRATTAMENTO E MONITORAGGIO DEI RISCHI	16
9. INFORMAZIONE COME RISORSA AZIENDALE	17
10. MISURE PER IL PERSONALE DIPENDENTE	18
10.1. FORMAZIONE E CONSAPEVOLEZZA	18
11. CLASSIFICAZIONE DELLE INFORMAZIONI	19
11.1. PRINCIPI GENERALI	19
11.2. CRITERI DI CLASSIFICAZIONE	20
11.3. CONSERVAZIONE DELLE INFORMAZIONI	21
11.3.1. CANCELLAZIONE DEI DATI	21
11.3.2. MISURE PER I CLIENTI	22
11.4. TRASFERIMENTO DELLE INFORMAZIONI	22
11.4.1. TRASMISSIONE SICURA SU RETI PUBBLICHE	22
11.4.2. CONDIVISIONE DEI DATI	22
11.4.3. SUPPORTI RIMOVIBILI	22
11.5. MISURE DI SICUREZZA ADEGUATE	23
11.5.1. INFORMAZIONI PUBBLICHE	23
11.5.2. INFORMAZIONI AD USO INTERNO	23

11.5.3.	INFORMAZIONI CONFIDENZIALI	23
11.5.4.	INFORMAZIONI SEGRETE	24
11.6.	MISURA DI SICUREZZA: LA CRITTOGRAFIA	25
12.	CONTROLLO DEGLI ACCESSI LOGICI	26
12.1.	PRINCIPI IN MATERIA DI CONTROLLO DEGLI ACCESSI	26
12.2.	UTENZE.....	26
12.3.	ASSEGNAZIONE, MODIFICA E REVOCA DELLE UTENZE DI DOMINIO.....	27
12.4.	AMMINISTRATORI DI SISTEMA	27
12.5.	ACCESSO AI SISTEMI DEI CLIENTI	28
12.6.	ACCESSO DEI CLIENTI AL CLOUD GPI	28
12.7.	UTENZE DEI CLIENTI	28
13.	CONTROLLO DEGLI ACCESSI FISICI	28
13.1.	MISURE DI SICUREZZA DEGLI ACCESSI	29
14.	SVILUPPO SICURO DEL SOFTWARE	29
14.1.	CICLO DI SVILUPPO.....	30
15.	GESTIONE DELL'INFRASTRUTTURA	31
15.1.	NETWORKING.....	32
15.2.	BACKUP	32
15.3.	CONTINUITA' OPERATIVA	33
15.4.	CESSAZIONE DEL SERVIZIO CLOUD	34
16.	MONITORAGGIO DEI SISTEMI	35
16.1.	VULNERABILITY MANAGEMENT	35
16.2.	GESTIONE DELLE POSTAZIONI DI LAVORO.....	37
16.3.	GESTIONE DEI LOG	37
17.	GESTIONE DEGLI INCIDENTI	38
17.1.	RUOLI E RESPONSABILITÀ	39
17.2.	LE FASI DI INCIDENT RESPONSE	40
17.2.1.	LA FASE DI RILEVAZIONE E ANALISI	40
17.2.1.1.	CRITICITÀ E CLASSIFICAZIONE DEGLI INCIDENTI.....	41
17.2.2.	LA FASE DI GESTIONE DEGLI INCIDENTI.....	42
17.2.2.1.	CONTENIMENTO.....	42

17.2.2.2.	ERADICATION.....	42
17.2.3.	RECUPERO.....	43
17.3.	ANALISI POST – INCIDENTE E MIGLIORAMENTO CONTINUO	44
17.4.	DATA BREACH	44
17.4.1.	SCHEMA DI VALUTAZIONE DEGLI SCENARI	45
17.4.2.	SCENARI DI NOTIFICA ALL'AUTORITÀ GARANTE	46
17.4.2.1.	MODALITÀ DI NOTIFICA DELLA VIOLAZIONE.....	47
17.4.3.	SCENARI DI NOTIFICA ALL'INTERESSATO.....	47
17.4.3.1.	MODALITÀ DI NOTIFICA DELLE VIOLAZIONI ALL'INTERESSATO	47
17.5.	REGISTRO DEGLI INCIDENTI E DATA BREACH	48
18.	GESTIONE DELLA CONTINUITÀ OPERATIVA.....	48
18.1.	RUOLI.....	48
18.2.	BIA E RISK ASSESSMENT	48
18.3.	SCENARI DI BUSINESS CONTINUITY	49
18.4.	MISURE PREVENTIVE.....	49
18.5.	LE FASI DI GESTIONE DELL'INCIDENTE	50
18.6.	TEST E SIMULAZIONI PERIODICHE	50
19.	PRIVACY POLICY	51
19.1.	PRINCIPI GENERALI.....	51
19.2.	TRATTAMENTO DEI DATI PERSONALI	53
19.3.	FINALITÀ DEL TRATTAMENTO.....	53
19.4.	INFORMATIVA	54
19.5.	RESPONSABILIZZAZIONE	54
19.5.1.	METODOLOGIA SULLE ATTIVITÀ DI TRATTAMENTO	55
19.6.	DIRITTI DEGLI INTERESSATI	55
19.7.	DPIA.....	56
19.8.	REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO.....	56
20.	GESTIONE DEI FORNITORI	57
21.	VERIFICA E MONITORAGGIO.....	57
22.	DOCUMENTAZIONE.....	58
23.	MIGLIORAMENTO CONTINUO	58