

# PIANO DI SICUREZZA E CONTINUITÀ - STAKEHOLDER

| Redazione     | Approvazione di Funzione | Approvazione Head of Compliance & Quality Assurance |
|---------------|--------------------------|-----------------------------------------------------|
| Alex Bertoldi | Roberto Conci            | Marco Di Domenico                                   |
| 05/10/2026    | 05/10/2026               | 05/10/2026                                          |

## 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<br>Aggiunto il paragrafo relativo ai fornitori |
| 1.2      | 22/04/2025 | 12.6, 12.7,<br>15, 15.1,<br>15.4 | Aggiornamento dei paragrafi indicati                                                                                          |
| 1.3      | 17/07/2025 | 7.1; 11.4.3;<br>11.4.4           | Aggiornamento dei paragrafi                                                                                                   |
| 1.4      | 05/10/2026 | -                                | Correzione refusi                                                                                                             |
|          |            |                                  |                                                                                                                               |
|          |            |                                  |                                                                                                                               |

## SOMMARIO

|                                                        |    |
|--------------------------------------------------------|----|
| 1. SCOPO .....                                         | 8  |
| 2. CAMPO DI APPLICAZIONE .....                         | 8  |
| 3. NORMATIVA .....                                     | 8  |
| 4. CERTIFICAZIONI E POLITICHE .....                    | 8  |
| 5. APPROCCIO ALLA SICUREZZA DELLE INFORMAZIONI .....   | 12 |
| 6. STRATEGIA AZIENDALE.....                            | 12 |
| 6.1. IL CICLO DI VITA DELLA CYBERSECURITY .....        | 13 |
| 7. RUOLI E RESPONSABILITÀ .....                        | 13 |
| 7.1. ASSEGNAZIONE DELLE RESPONSABILITÀ .....           | 16 |
| 7.1.1. RESPONSABILITÀ DELL'ORGANIZZAZIONE .....        | 16 |
| 7.1.2. RESPONSABILITÀ DEI SOGGETTI ESTERNI .....       | 17 |
| 7.1.3. RESPONSABILITÀ DELLE AMMINISTRAZIONI TERZE..... | 17 |
| 8. ANALISI DEI RISCHI .....                            | 17 |
| 8.1. IDENTIFICAZIONE DEI RISCHI .....                  | 17 |
| 8.1.1. IDENTIFICAZIONE DELLE MINACCE .....             | 18 |
| 8.1.2. VALUTAZIONE DEI RISCHI.....                     | 18 |
| 8.2. VALUTAZIONE DELLE VULNERABILITÀ DEI SISTEMI ..... | 19 |
| 8.3. TRATTAMENTO E MONITORAGGIO DEI RISCHI .....       | 19 |
| 9. INFORMAZIONE COME RISORSA AZIENDALE.....            | 20 |
| 10. MISURE PER IL PERSONALE DIPENDENTE .....           | 20 |
| 10.1. FORMAZIONE E CONSAPEVOLEZZA .....                | 21 |
| 11. CLASSIFICAZIONE DELLE INFORMAZIONI .....           | 21 |
| 11.1. PRINCIPI GENERALI.....                           | 22 |
| 11.2. CRITERI DI CLASSIFICAZIONE .....                 | 22 |
| 11.3. CONSERVAZIONE DELLE INFORMAZIONI .....           | 23 |
| 11.3.1. CANCELLAZIONE DEI DATI .....                   | 24 |
| 11.3.2. MISURE PER I CLIENTI .....                     | 24 |
| 11.4. TRASFERIMENTO DELLE INFORMAZIONI .....           | 25 |
| 11.4.1. TRASMISSIONE SICURA SU RETI PUBBLICHE .....    | 25 |
| 11.4.2. CONDIVISIONE DEI DATI.....                     | 25 |

|         |                                                              |    |
|---------|--------------------------------------------------------------|----|
| 11.4.3. | SUPPORTI RIMOVIBILI .....                                    | 25 |
| 11.4.4. | DOCUMENTI CARTACEI .....                                     | 25 |
| 11.5.   | MISURE DI SICUREZZA ADEGUATE.....                            | 26 |
| 11.5.1. | INFORMAZIONI PUBBLICHE .....                                 | 26 |
| 11.5.2. | INFORMAZIONI AD USO INTERNO .....                            | 26 |
| 11.5.3. | INFORMAZIONI CONFIDENZIALI.....                              | 26 |
| 11.5.4. | INFORMAZIONI SEGRETE .....                                   | 27 |
| 11.6.   | MISURA DI SICUREZZA: LA CRITTOGRAFIA .....                   | 28 |
| 12.     | CONTROLLO DEGLI ACCESSI LOGICI .....                         | 29 |
| 12.1.   | PRINCIPI IN MATERIA DI CONTROLLO DEGLI ACCESSI .....         | 29 |
| 12.2.   | UTENZE.....                                                  | 29 |
| 12.3.   | ASSEGNAZIONE, MODIFICA E REVOCA DELLE UTENZE DI DOMINIO..... | 30 |
| 12.4.   | AMMINISTRATORI DI SISTEMA .....                              | 30 |
| 12.5.   | ACCESSO AI SISTEMI DEI CLIENTI .....                         | 31 |
| 12.6.   | ACCESSO DEI CLIENTI AL CLOUD GPI .....                       | 31 |
| 12.7.   | UTENZE DEI CLIENTI .....                                     | 31 |
| 13.     | CONTROLLO DEGLI ACCESSI FISICI .....                         | 31 |
| 13.1.   | MISURE DI SICUREZZA DEGLI ACCESSI .....                      | 32 |
| 14.     | SVILUPPO SICURO DEL SOFTWARE .....                           | 32 |
| 14.1.   | CICLO DI SVILUPPO.....                                       | 33 |
| 15.     | GESTIONE DELL'INFRASTRUTTURA .....                           | 34 |
| 15.1.   | NETWORKING.....                                              | 35 |
| 15.2.   | BACKUP .....                                                 | 35 |
| 15.3.   | CONTINUITA' OPERATIVA .....                                  | 36 |
| 15.4.   | CESSAZIONE DEL SERVIZIO CLOUD .....                          | 37 |
| 16.     | MONITORAGGIO DEI SISTEMI .....                               | 38 |
| 16.1.   | VULNERABILITY MANAGEMENT .....                               | 38 |
| 16.2.   | GESTIONE DELLE POSTAZIONI DI LAVORO.....                     | 40 |
| 16.3.   | GESTIONE DEI LOG .....                                       | 40 |
| 17.     | GESTIONE DEGLI INCIDENTI .....                               | 41 |
| 17.1.   | RUOLI E RESPONSABILITÀ .....                                 | 42 |

|           |                                                            |    |
|-----------|------------------------------------------------------------|----|
| 17.2.     | LE FASI DI INCIDENT RESPONSE .....                         | 43 |
| 17.2.1.   | LA FASE DI RILEVAZIONE E ANALISI.....                      | 43 |
| 17.2.1.1. | CRITICITÀ E CLASSIFICAZIONE DEGLI INCIDENTI .....          | 44 |
| 17.2.2.   | LA FASE DI GESTIONE DEGLI INCIDENTI .....                  | 45 |
| 17.2.2.1. | CONTENIMENTO .....                                         | 45 |
| 17.2.2.2. | ERADICATION .....                                          | 46 |
| 17.2.3.   | RECUPERO .....                                             | 46 |
| 17.3.     | ANALISI POST – INCIDENTE E MIGLIORAMENTO CONTINUO .....    | 47 |
| 17.4.     | DATA BREACH .....                                          | 47 |
| 17.4.1.   | SCHEMA DI VALUTAZIONE DEGLI SCENARI.....                   | 48 |
| 17.4.2.   | SCENARI DI NOTIFICA ALL'AUTORITÀ GARANTE.....              | 49 |
| 17.4.2.1. | MODALITÀ DI NOTIFICA DELLA VIOLAZIONE .....                | 50 |
| 17.4.3.   | SCENARI DI NOTIFICA ALL'INTERESSATO .....                  | 50 |
| 17.4.3.1. | MODALITÀ DI NOTIFICA DELLE VIOLAZIONI ALL'INTERESSATO..... | 51 |
| 17.5.     | REGISTRO DEGLI INCIDENTI E DATA BREACH .....               | 51 |
| 18.       | GESTIONE DELLA CONTINUITÀ OPERATIVA.....                   | 51 |
| 18.1.     | RUOLI.....                                                 | 51 |
| 18.2.     | BIA E RISK ASSESSMENT .....                                | 52 |
| 18.3.     | SCENARI DI BUSINESS CONTINUITY .....                       | 52 |
| 18.4.     | MISURE PREVENTIVE.....                                     | 53 |
| 18.5.     | LE FASI DI GESTIONE DELL'INCIDENTE .....                   | 53 |
| 18.6.     | TEST E SIMULAZIONI PERIODICHE .....                        | 54 |
| 19.       | PRIVACY POLICY .....                                       | 54 |
| 19.1.     | PRINCIPI GENERALI.....                                     | 54 |
| 19.2.     | TRATTAMENTO DEI DATI PERSONALI .....                       | 56 |
| 19.3.     | FINALITÀ DEL TRATTAMENTO.....                              | 56 |
| 19.4.     | INFORMATIVA .....                                          | 57 |
| 19.5.     | RESPONSABILIZZAZIONE .....                                 | 58 |
| 19.5.1.   | METODOLOGIA SULLE ATTIVITÀ DI TRATTAMENTO.....             | 58 |
| 19.6.     | DIRITTI DEGLI INTERESSATI .....                            | 58 |
| 19.7.     | DPIA.....                                                  | 59 |

|       |                                             |    |
|-------|---------------------------------------------|----|
| 19.8. | REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO..... | 60 |
| 20.   | GESTIONE DEI FORNITORI .....                | 60 |
| 21.   | VERIFICA E MONITORAGGIO.....                | 61 |
| 22.   | DOCUMENTAZIONE.....                         | 61 |
| 23.   | MIGLIORAMENTO CONTINUO .....                | 61 |