COMUNE DI SAN MICHELE DI GANZARIA
Via Roma, 82/84 - Cap. 95040, cap 95040– San Michele di Ganzaria (CT)
Codice Fiscale 82002180873 Partita IVA 01180410878 – Tel (+39) 0933 971011
Mail: segreteria@comune.sanmichelediganzaria.ct.it
PEC: prot.gen@pec.comune.sanmichelediganzaria.ct.it

# # #

Playbook sulle Procedure di back up, ripristino e sicurezza dei sistemi

# # #

1. Titolo e Versione

- **Titolo:** *Procedure di back up, ripristino e sicurezza dei sistemi*
- **Versione:** 1.0 del 04/02/2026 – approvato dall'amministrazione con delibera GC n 28 del 20/03/2026.

---

2. Descrizione

Il presente Playbook definisce le **misure tecniche e organizzative** necessarie per garantire un livello di sicurezza adeguato al rischio, assicurando su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi di trattamento. L'obiettivo principale è regolamentare le procedure di salvataggio (back-up), ripristino e protezione dei dati personali per prevenire perdite, distruzioni o accessi non autorizzati.

---

3. Condizioni di attivazione

L'esecuzione delle procedure previste è determinata dai seguenti eventi e logiche di rilevamento:

- **Intervalli temporali predefiniti:**
  - **Cadenza settimanale:** verifica aggiornamenti del sistema operativo.
  - **Cadenza ogni 8 giorni (o giornaliera):** esecuzione del back-up sistematico dei dati.
  - **Cadenza quindicinale:** svuotamento del cestino dei file cancellati.
  - **Cadenza mensile:** verifica del corretto funzionamento dei programmi di back-up e dell'integrità dei file.
  - **Cadenza semestrale:** audit sull'efficacia delle misure tecniche e organizzative e simulazione di ripristino.
- **Segnalazioni di sistema:** rilevamento di anomalie da parte dell'antivirus o disponibilità di nuovi aggiornamenti software.
- **Trattamento di categorie particolari di dati:** invio di dati ex art. 9 e 10 Reg. UE 679/2016 che richiede cifratura obbligatoria.
- **Incidente fisico o tecnico:** necessità di ripristinare tempestivamente l'accesso ai dati a seguito di un malfunzionamento.

---

4. Attività

Fase 1: Manutenzione e Igiene Digitale

- Effettuare periodicamente l'**aggiornamento del sistema operativo** (almeno una volta a settimana) e dell'antivirus.
- Accedere alla rete preferibilmente in **navigazione in incognito** ed evitare il download di programmi privi di licenza o applicazioni non necessarie.
- Verificare periodicamente il funzionamento del **gruppo di continuità**.

Fase 2: Gestione e Organizzazione dei Dati

- Organizzare i file in cartelle ordinate (criterio alfabetico, cronologico, ecc.) e rinominarli in modo identificabile.
- Eliminare file duplicati o sovrabbondanti e correggere dati incompleti.
- Applicare, ove possibile, la **cifratura**, la **pseudonimizzazione** o codici convenzionali per ridurre la sensibilità dei dati.

Fase 3: Operazioni di Back-up e Archiviazione

- Eseguire il **back-up sistematico** (almeno ogni 8 giorni).
- Annotare data e ora dell'ultimo salvataggio in un **registro storico** (cartaceo o fuori rete).
- Conservare i supporti rimovibili in luoghi sicuri, come **cassaforti o cassetti chiusi a chiave**.

Fase 4: Sicurezza delle Comunicazioni (Email/PEC)

- Inserire di default avvertenze sulla riservatezza nei messaggi in uscita.
- Cifrare i file contenenti dati sensibili con **password robusta** (almeno 8 caratteri alfanumerici e speciali) da comunicare per altra via (es. telefono).
- Utilizzare la copia conoscenza nascosta (CCN) per invii a più destinatari privati.
- **Filtrare le mail sospette:** non aprire allegati o link se il mittente è sconosciuto, se l'italiano è scorretto o se l'estensione del file è insolita (es. .exe, .sys, o file compressi).

Fase 5: Monitoraggio e Verifica

- Eseguire test mensili di integrità dei file di back-up.
- Simulare ogni sei mesi un'attività di **ripristino dei dati** per testare la resilienza del sistema.

---

5. Ruoli e Responsabilità (Matrice RASCI)

Attività	Titolare (Sindaco)	RPD (DPO)	Funzionario/ Dirigente di Area	Dipendenti Autorizzati	Designato Sicurezza sistemi /Amm. Di sistema
Definizione e aggiornamento procedure	**A**	**C/I**	**R**	**S**	**S**
Esecuzione back-up e aggiornamenti	**A**	**-**	**S**	**R**	**S**
Gestione sicura email e file	**A**	**C**	**S**	**R**	**S**
Verifica mensile integrità back-up	**A**	**-**	**S**	**R**	**S/I**
Audit semestrale e test ripristino	**A**	**I**	**R**	**S**	**R**
Segnalazione criticità post-verifica	**A**	**I/C**	**R**	**S**	**R**

Legenda:

- **R (Responsible):** Chi esegue l'attività. Tutti i soggetti autorizzati sono responsabili dell'applicazione quotidiana delle misure di sicurezza.
- **A (Accountable):** Chi ha la responsabilità ultima. Il Titolare deve essere in grado di dimostrare la conformità (principio di *accountability*).
- **S (Support):** Chi supporta l'esecuzione (es. organi gestionali per le risorse o personale designato).
  - **Designato:** Saitta Antonio
- **C (Consulted):** Chi fornisce pareri esperti (es. il RPD per la valutazione dell'efficacia delle misure).
- **I (Informed):** Chi deve essere informato dei risultati o dell'esistenza delle procedure.

6. Rinvio alle Istruzioni operative per il personale

Salvo quanto previsto nel presente playbook, rimane applicabile quanto già previsto nelle ***Istruzioni operative per il personale autorizzato al trattamento dei dati personali*** già approvate dall'amministrazione con deliberaa G.M. n. 122 del 24.12.2019,

Nota: La mancata conformità a queste regole può comportare provvedimenti disciplinari per i dipendenti o la risoluzione dei contratti per le terze parti.