# C O M U N E D I O L B I A

*Settore AA.GG. e Provveditorato - Servizio ITC*

# ALLEGATO MISURE DI SICUREZZA ICT

## SERVIZIO "CENTRO DISABILITÀ GLOBALE" E SPORTELLO SEGRETARIATO SOCIALE

## GESTIONE PLUS 2025-2027

Il Fornitore si impegna ad adottare le seguenti misure di sicurezza:

- misure di cifratura dei dati personali (punti 2, 4, 6);
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (punti C.1.2, 2, 3, 5, 7);
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (punto 3);
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (punto 3);
- misure di identificazione e autorizzazione dell'utente (punto 4);
- misure di protezione dei dati durante la trasmissione, durante la conservazione, misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati (punto 6);
- misure per garantire la registrazione degli eventi (punto 4.2, 4.5);
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita (punto 4);
- misure di informatica interna e di gestione e governance della sicurezza informatica (punti 1.2, 2, 3, 4, 5, 6, 7, 8);
- misure per garantire la minimizzazione dei dati (punto A 1.1);
- misure per garantire la qualità dei dati (punti 7 e 8);
- misure per consentire la portabilità dei dati e garantire la cancellazione (punto 8.4, 8.5).

Nelle tabelle sottostanti sono riportate in concreto le misure di sicurezza ICT da mettere in atto.

| | | |
|---|---|---|
| A. | *DATI GENERALI* | |
| | **1.1. Banche dati e superficie di attacco (***relativi ai soli dati necessari e non eccedenti lo scopo del trattamento***)**<br>Banca dati anagrafica cittadini e dei relativi nuclei familiari.<br>Banca dati sanitari.<br>Banca dati informazioni economiche e lavorative. | |
| | **1.2. Tipologia connessione \| interventi remoti**<br>FTTPs, HTTPS, VPN, SSH. | |
| | **1.3. Interventi in sede**<br>SI | |

| | | |
|---|---|---|
| *B.* | *MISURE ADEGUATE INTERNE ALLA RETE DEL TITOLARE* | |
| | 1.1. I responsabili che verranno nominati saranno tenuti ad attenersi al Regolamento ed al Manuale degli Amministratori di Sistema | |
| *C.* | *MISURE ADEGUATE SU AMBIENTE RESPONSABILE* | |
| | 1. INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI | |
| | 1.2. Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione. | |



Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220

| | | |
|---|---|---|
| 2. | PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER | |
| | 2.1. Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). | |
| | 2.2. Dispositivi come telefoni cellulari, tablet, laptop, dischi esterni, chiavette USB, Schede SD e altri dispositivi elettronici portatili che memorizzano o elaborano dati dell'Ente, devono essere criptati. | |

| | | |
|---|---|---|
| 3. | VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ | |
| | 3.1. Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). | |

| | | |
|---|---|---|
| 4. | USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE | |
| | 4.1. Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi. | |
| | 4.2. Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | |
| | 4.3. Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. | |
| | 4.4. Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso. | |
| | 4.5. Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa. | |
| | 4.6. Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri). | |
| | 4.7. Impedire che per le utenze amministrative vengano utilizzate credenziali deboli. | |
| | 4.8. Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging). | |
| | 4.9. Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | |
| | 4.10. Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. | |
| | 4.11. Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | |
| | 4.12. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso. | |
| | 4.13. Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio). | |
| | 4.14. Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza. | |
| | 4.15. Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | |

| | | |
|---|---|---|
| 5. | DIFESE CONTRO I MALWARE | |
| | 5.1. Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. | |
| | 5.2. Installare su tutti i dispositivi firewall ed IPS personali. Per i dispositivi all'interno di una rete dati, deve essere implementata la difesa attraverso Firewall e IPS centralizzati. | |
| | 5.3. Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati. | |
| | 5.4. Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. | |
| | 5.5. Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host. | |
| | 5.6. Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione. | |




Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220

| | | |
|---|---|---|
| | 5.7. Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | |
| | 5.8. Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | |
| | 5.9. Disattivare l'apertura automatica dei messaggi di posta elettronica. | |
| | 5.10. Disattivare l'anteprima automatica dei contenuti dei file. | |
| | 5.11. Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. | |
| | 5.12. Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam. | |
| | 5.13. Filtrare il contenuto del traffico web. | |
| | 5.14. Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab). | |

| | | |
|---|---|---|
| | 6. TRASMISSIONE TELEMATICA DI DOCUMENTAZIONE | |
| | 6.1. La trasmissione telematica di un documento digitale a mezzo di PEC, E-Mail , FTPs, HTTPs, Cisco WebEX, dovrà essere eseguita inviando la copia criptata del documento: la password/chiave per decifrare dovrà essere inviata separatamente con altra comunicazione. | |
| | 6.2. Qualunque altro mezzo di trasmissione si voglia utilizzare, diverso da quelli indicati al punto 6.1, dovrà essere autorizzato dal responsabili ICT dell'Ente. | |

| | | |
|---|---|---|
| | 7 COPIE DI DATI | |
| | 7.1. Non è autorizzata alcuna copia (totale o parziale) dei dati del Comune di Olbia presso la vs. organizzazione, neanche per test interni. | |
| | 7.2. Qualsiasi copia del/dei DB server andrà fatta, se necessario, in locale e lasciata sugli apparati del Comune. | |
| | 7.3. Non è autorizzato il trasferimento files da desktop utente, contenente qualsivoglia dato personale. | |
| | 7.4. Non sono autorizzati i trasferimenti su cloud di documenti contenenti dati di utenti del Comune di Olbia o dei dati presenti sui database ai quali la vs. società ha accesso. | |
| | 7.5. Si richiede la distruzione (con metodi sicuri, autorizzati e supervisionati dal Comune di Olbia) di eventuali dati in vs. possesso che vadano oltre le finalità del contratto in essere con il Comune.<br>Tale attività di cancellazione dovrà essere comunicata (*con indicazione dei processi e metodi utilizzati*) alla PEC istituzionale: protocollo@pec.comuneolbia.it | |

| | | |
|---|---|---|
| | 8. ALTRE ATTIVITA' | |
| | 8.1. Pseudonimizzazione dei dati all'interno dei server dell'Amministrazione (a livello di database). | |
| | 8.2. Interfaccia WEB di eventuale applicazione accessibile solo tramite SSL. | |
| | 8.3. Certificazione che tutta la vs. suite sia GDPR compliant, soprattutto che sia compliant per PrivacyByDesign | |
| | 8.4. Alla chiusura del contratto deve essere garantito il punto 7.5, riguardante la distruzione di eventuali dati in vs. possesso, contenenti qualsivoglia dato personale. | |
| | 8.5. Normalizzazione struttura banca dati per esportazione e disponibilità del dato senza interruzioni/perdite, secondo gli standard. | |

Il Fornitore

(*Documento Firmato Digitalmente*)




Via Dante, 1 – 07026 OLBIA (OT) Tel.0789/52220