ALLEGATO F - MISURE DI SICUREZZA PER LA PROTEZIONE DEI DATI DI CWBT
AI SENSI DEL REGOLAMENTO EUROPEO 679/2016

REVISIONI	VERS.	DATA	DESCRIZIONE	AUTORE
	1	03/03/2023	Prima stesura	Roberto Martina
	2	30/07/2025	Seconda stesura	Roberto Martina
	3	23/06/2026	Terza stesura	Roberto Martina

VALIDATO DA	Roberto Martina	**DATA** 23/06/2026	**FIRMA**
APPROVATO DA	Roberto Martina	**DATA** 23/06/2026	**FIRMA**

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

INDICE

1. SCOPO 3

2. AMBITO 3

3. POLICY 3

4. GENERALE 3

5. GESTIONE DEGLI ACCESSI 3

6. SICUREZZA FISICA 4

7. SICUREZZA DI RETI, SISTEMI E DISPOSITIVI 4

8. SICUREZZA DEI DATI 4

9. LOGGING E MONITORING 5

10. BACKUP, BUSINESS CONTINUITY E DISASTER RECOVERY 5

11. SECURITY E PRIVACY BY DESIGN E BY DEFAULT 5

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

1. SCOPO

CWBT pone regole restrittive atte a proteggere dalla perdita, modifica, divulgazione non autorizzata o accesso in modo accidentale o illegale i dati personali trasmessi, conservati o comunque trattati.
Questa policy ha l'obiettivo primario di diffondere consapevolezza ed evitare scenari di perdita accidentale evidenziando i requisiti per la prevenzione di scenari di data breach.

2. AMBITO

Questa policy si applica ai dati dei clienti, ai dati personali o altri dati della compagnia classificabili come sensibili. E dunque si applica ad ogni server, database e sistema IT che gestisce questi dati, incluso ogni dispositivo che viene regolarmente usato per le mail, gli accessi web, o altre mansioni lavorative. Inoltre, ricadono sotto questa policy, tutti gli utenti che utilizzano i servizi IT di CWBT.

3. POLICY

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità (sub-fornitori) ed abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso.

4. GENERALE

Gli utenti devono essere associati ad ID che li rendano identificabili e responsabili per le loro azioni.

Evidenze sull'accesso degli utenti possono essere utilizzati per fornire informazioni utili ad eventuali investigazioni.

CWBT adotta un processo di IT Security & Risk Assessment per identificare, valutare e trattare i rischi ICT. Il processo è riesaminato almeno annualmente e/o al verificarsi di cambiamenti significativi (architettura, fornitori critici, data location).
Output minimi: registro rischi e piano remediation con priorità e scadenze, approvato dal management.

5. GESTIONE DEGLI ACCESSI

- L'accesso ai servizi IT dell'azienda deve essere concesso tramite ID assegnato e password complessa. Gli account devono essere forniti dal reparto IT e ne deve essere tenuta traccia dall'HR;
- le password devono essere formulate sulla base dalle linee guida NIST (Digital Identity Guidelines) e gestite tramite appositi tool di password management;
- gli accessi devono essere concessi secondo il principio del privilegio minimo e della segregation of duties, concedendo al personale e ai programmi le autorizzazioni minime e necessarie a completare i loro specifici task;
- il reparto IT inoltre monitora l'utilizzo degli ID con cadenza settimanale;
- il reparto IT si occupa della dismissione di un account non più necessario causa trasferimento ad altra mansione, dimissioni o licenziamento;
- al termine di ogni sessione deve essere effettuato il log-out e lo spegnimento dei dispositivi.

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

- Gli accessi privilegiati (amministratori di sistema e account con privilegi elevati) sono limitati al minimo necessario, protetti con controlli rafforzati e soggetti a tracciamento dedicato. È prevista una procedura di accesso di emergenza (break-glass) con tracciamento e revisione ex-post. Le verifiche periodiche delle utenze includono anche gli account privilegiati.

6. SICUREZZA FISICA

- Documenti contenenti dati personali devono essere immediatamente rimossi dalle fotocopiatrici una volta utilizzati;
- l'uso di fotocopiatrici su documenti contenenti dati personali deve essere concesso solo su autorizzazione;
- la documentazione deve essere rinchiusa in contenitori dotati di serratura quando non utilizzata;
- lo schermo dei dispositivi deve essere tenuto in modalità blocca schermo protetto da password quando non in uso;
- l'accesso alle sedi di persone esterne all'organizzazione deve essere concesso in apposite partizioni della struttura;
- in via generale deve essere tenuta una politica di clean e clear desk nell'utilizzo di documentazione contenente dati di titolarità/responsabilità di CWBT;
- devono essere adottati protocolli di distruzione-sicura della documentazione cartacea (tramite strumenti di shredding) contenente dati di titolarità/responsabilità CWBT.

7. SICUREZZA DI RETI, SISTEMI E DISPOSITIVI

- Il personale deve essere formato e informato sulle modalità di attacco informatico, protezione delle reti e dei dispositivi e modalità di aggiornamento sicura di un sistema;
- devono essere tenute tecnologie di prevenzione atte a mitigare il rischio di attacchi mirati a sottrarre dati/ bloccare i sistemi come anti-virus o anti-malware;
- i dispositivi devono essere regolarmente soggetti a patching per risolvere situazioni di vulnerabilità o conflitti;
- devono essere svolti test di sicurezza periodici e strutturati (VAPT) ed eventuali vulnerabilità devono essere risolte tempestivamente;
- gli ambienti di test di sviluppo, pre-produzione e produzione devono essere separati;
- è necessario garantire politiche di deny-by-default per il controllo del traffico di rete in entrata;
- adeguate tecnologie di sicurezza devono essere adottate per il controllo e le analisi del traffico di rete in entrata ed uscita (es. firewall, WAF, IDS/IPS).

8. SICUREZZA DEI DATI

- Deve essere assicurata l'anonimizzazione dei dati in fase di test, sviluppo e pre-produzione. L'utilizzo di dati in chiaro è consentito in casi eccezionali solo per finalità specifiche e solo se preventivamente autorizzato;
- devono essere disabilitati secondo il principio della security by default quelle funzionalità o protocolli che possano creare disclosure non autorizzate di dati;
- l'utilizzo di dispositivi e media portatili deve essere preventivamente autorizzato dall'Azienda, i contenuti di dispositivi e media portatili devono essere cifrati;
- l'utilizzo di dispositivi che possano portare all'esterno dell'azienda dati di titolarità/responsabilità CWBT deve essere preventivamente approvato da CWBT e sottoposto ad opportune misure di sicurezza/cifratura;
- file di log e backup devono essere contrassegnati da timestamp, archiviati in maniera sicura ed accessibili solo da personale autorizzato;
- il personale o i fornitori di CWBT che hanno accesso remoto al network di CWBT deve essere autenticato tramite VPN;
- deve essere perseguita la segregazione delle reti ove questo non risulti tanto gravoso da impedire il perseguimento della mission aziendale;.
- devono essere adottati strumenti e tecnologie di sicurezza volti a monitorare/controllare il flusso di dati personali da reti interne verso reti esterne;
- i canali di comunicazione e/o i flussi dati e/o i dati stessi (es. file protetto da password) verso reti esterne devono essere cifrati al fine di proteggere i dati personali in transito;
- dati at rest devono essere cifrati all'interno di storage/ambienti Cloud;

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.

- deve essere adottato un sistema standard per la gestione delle chiavi di cifratura.
- devono essere adottati processi e protocolli di cancellazione: sicura (es. wiping o cifratura irreversibile) al termine del ciclo di vita del dato (data deletion/disposal a seguito dello scadere del tempo di retention) e/o in fase di restituzione di asset e dispositivi aziendali.

9. LOGGING E MONITORING

- È richiesto il logging degli accessi del personale interno ed esterno ai sistemi di produzione che processano dati personali.
- Il logging include almeno: identificativo utente, timestamp, esito, sistema interessato e sorgente. Per gli accessi privilegiati è previsto tracciamento dedicato e revisione periodica dei log. I log sono conservati con accesso controllato e retention definita internamente.

10. BACKUP, BUSINESS CONTINUITY E DISASTER RECOVERY

- Deve essere predisposto un piano di disaster recovery, che contempli un sito alternativo, come raggiungerlo e la dotazione e la struttura utili a ripristinare e proseguire la continuità aziendale;
- devono essere predisposti backup da conservare e in caso di danneggiamento degli stessi o degli strumenti elettronici a supporto deve essere garantito in tempi compatibili con i diritti degli interessati.
- Frequenze di backup, retention e obiettivi di ripristino sono definiti in funzione della criticità e degli obiettivi RTO/RPO applicabili (definiti nei piani BCP/DRP e, per i servizi Cliente, nei relativi profili service-specific). In caso di incidente cyber, il ripristino privilegia copie consistenti e verifiche di integrità prima del rientro in esercizio.

11. SECURITY E PRIVACY BY DESIGN E BY DEFAULT

Devono essere adottati controlli specifici di security e privacy by design/default nell'ambito dei principali processi IT di business.

12. TERZE PARTI / SUBFORNITURA

CWBT governa i rischi derivanti da terze parti tramite valutazioni di sicurezza sui fornitori critici. In caso di subfornitura rilevante, CWBT applica un processo di valutazione e garantisce requisiti di sicurezza equivalenti nei subcontratti, nel rispetto degli obblighi contrattuali verso il Cliente.

Codice Web Banking Technology – CF/PI: 03577200987 https://www.cwbt.it
Via Venezia, 92/b – 35131 Padova (PD) info@cwbt.it

Tutte le informazioni riportate nel presente documento non possono essere utilizzate in toto o in parte, né cedute o riprodotte senza il permesso scritto.