Policy Sicurezza Informatica ai fini della Privacy

1. PREMESSA

Il presente documento definisce gli standard dell'**"Associazione Banco Alimentare della Sicilia O.N.L.U.S."** (da ora in poi "**Banco"**) inerenti la Protezione dei Dati e il loro Trattamento in relazione all'utilizzo di Hardware e Software, al fine di garantire un adeguato livello di protezione delle informazioni di qualsiasi tipo, compresi i dati personali.

Questa policy è diretta a tutti gli Operatori del Banco a qualsiasi livello funzionale (Dipendenti, Volontari, Tirocinanti, Fornitori di Servizi, Consulenti, ecc.) per i quali costituisce un ambito Culturale, una Guida e una Condotta per la Protezione dei Dati.

La presente informativa è rivolta anche a tutti gli Utenti del Banco come dimostrazione della politica di Sicurezza, Trasparenza, Protezione, Integrità e Riservatezza sui Dati Acquisiti. (Art. 5 del G.D.P.R. 679/2016)

2. MISURE DI SICUREZZA

2.1. Misure di sicurezza individuali

Tutti gli Operatori sono tenuti a trattare le informazioni ricevute o generate a seguito di trattamento dei dati, con o senza l'ausilio di software, con la massima attenzione e tenendo conto della sicurezza e riservatezza: (Art. 5 c.1 lett. f del G.D.P.R. 679/2016)

a. **Protezione delle Credenziali di Accesso.** Le credenziali di autenticazione (nome utente e password) sono **strettamente personali** e non cedibili. Devono essere mantenute "***riservate*** e ***archiviate in modo sicuro***". Requisiti fondamentali per una buona password sono: un minimo di **8 caratteri alfanumerici, alternanza di lettere maiuscole e minuscole, presenza di almeno un carattere speciale** (***@#$%^&**), **non usare parole comuni** (come "password", QWERTY, 123456), **non usare la** data del proprio compleanno o quello dei familiari, **non usare** il proprio nome o quello dei familiari

o di animali domestici, **non usare** parole che si trovano sul dizionario, **non usare** la stessa password per tutto;

b. **Durata della Password**. Per una migliore sicurezza la password deve essere cambiata almeno una volta l'anno (ogni 6 mesi). Per l'accesso a dati particolari si raccomanda di cambiare la password ogni tre mesi;
c. Tutte le volte che si lascia la propria postazione di lavoro, il personal computer e/o notebook e/o tablet, devono essere bloccati per evitare di essere utilizzati da altri;
d. Tutte le volte che si lascia la propria postazione, eventuali documenti cartacei contenenti dati personali, devono essere riposti negli appositi armadi di sicurezza;
e. La stampa di documenti contenenti dati personali non deve essere inviata a stampanti che non siano sotto il proprio controllo visivo (stampanti condivise) per evitare che siano visti o presi da persone non autorizzate;
f. Non è consentito produrre copie di documenti informatici e/o cartacei, del Banco, di alcun tipo per uso personale;
g. Non è consentita la copia di alcun tipo di dato del Banco su dispositivi di memorizzazione personali quali ad esempio pendrive o su cloud personali. È vietato inoltre l'invio di e-mail personali non autorizzate;
h. I dispositivi mobili (notebook, tablet, smartphone, pendrive, hard disk esterni) che contengono Dati del Banco devono essere protetti contro lo smarrimento o furto attraverso l'utilizzo di un file system criptato;
i. Tutti i dispositivi devono essere aggiornati e protetti con antivirus e antimalware.

2.2. Misure di sicurezza per l'utilizzo di internet e della posta elettronica

Tutti i dispositivi dati in uso agli operatori dal Banco e dotate di connessione internet, potranno essere utilizzate solo per attività riconducibili direttamente alle finalità istituzionali.

a. Durante la navigazione in internet non dovranno essere visitati siti non inerenti le finalità istituzionali e comunque non riconducibili all'attività di lavoro;
b. Non è consentito l'utilizzo, in orario di lavoro, di strumenti personali per l'accesso ad internet;
c. Non è consentito l'uso di risorse personali (mail personali, dispositivi personali, ecc.) per lo svolgimento dei compiti istituzionali se non espressamente autorizzati;

d. l'account di posta elettronica del Banco deve essere utilizzato solo ed esclusivamente per lo svolgimento di attività istituzionali;
e. Gli allegati di posta elettronica ed i link presenti all'interno delle mail, devono essere aperti o attivati solo se si è certi e sicuri della provenienza. In tutti i casi dubbi, la mail deve essere inoltrata al responsabile dei servizi IT per una attenta analisi e valutazione;
f. L'inserimento in qualsiasi tipo di social network di informazioni personali o inerenti il Banco deve essere attentamente valutata e approvata per evitare la diffusione di dati riservati o che possano nuocere alle attività istituzionali del Banco. La mancata osservazione della prescrizione può comportare un'azione da parte del Titolare del Trattamento;

3. DOTAZIONE E USO DI BENI DEL BANCO

Il banco fornisce, al fine di consentire nel miglior modo possibile, per lo svolgimento dell'attività lavorativa, alcune dotazioni e beni aziendali tra i quali, a titolo esemplificativo, Personal Computer, Notebook, Smartphone in applicazione della politica delle risorse umane.

A tal proposito:

a. Nessun diritto può essere affermato dal lavoratore/volontario nei confronti del Banco su tali beni, a nessun titolo. Il lavoratore/volontario è responsabile e custode di quanto affidatogli ed è tenuto alla massima diligenza nel loro uso.
b. I beni informatici del Banco consegnati al lavoratore/volontario saranno configurati, impostati e predisposti secondo le direttive impartite dallo stesso. L'hardware e il software consegnati non potranno essere alterati senza previa e specifica autorizzazione, pertanto è vietato installare qualsiasi tipo di software o app, creare account e modificare password, senza precise direttive da parte del responsabile IT;
c. È vietato prestare a terzi, estranei alle attività del Banco, i beni in dotazione con particolare attenzione ai notebook e agli smartphone.

4. SMALTIMENTO E RIPARAZIONE DEI DISPOSITIVI INFORMATICI

I supporti informatici quali: notebbok, tablet, smartphone, hard disk e simili, contenenti informazioni e dati inerenti le attività istituzionali, devono essere smaltiti o inviati in riparazione in modo tale da evitare l'accesso da parte di persone non autorizzate.

5. MONITORAGGIO, REGISTRAZIONE, ATTIVITÀ DI AUDITING

Al fine di salvaguardare l'autenticità, l'integrità, la disponibilità e la riservatezza dei dati personali, viene effettuata attività di monitoraggio e registrazione degli accessi alle reti e ai sistemi informativi.

a. Gli accessi ai sistemi informatici vengono registrati e conservati per un periodo non superiore ai 6 mesi;
b. L'hardware e il software per l'archiviazione dei dati (NAS)registra e conserva i log di accesso che vengono conservati per un periodo di un anno;
c. Ai fini dell'applicazione delle norme relative alla suddetta policy, il Banco, può effettuare attività di auditing tramite il Responsabile Protezione Dati incaricato.

6. ADESIONE AL G.D.P.R. (Regolamento Generale sulla Protezione dei Dati)

L'**Associazione Banco Alimentare della Sicilia O.N.L.U.S** si è dotata di un Modello Organizzativo conforme al "Regolamento Generale sulla Protezione dei Dati" (G.D.P.R. 679/2016) di cui il presente documento è parte integrante.