Saronno Servizi
gestione servizi pubblici locali

Modello di Organizzazione, Gestione e Controllo

Adottato ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

PROTOCOLLO GESTIONE DEI SISTEMI INFORMATIVI

1. Introduzione

Il presente protocollo, in aggiunta ai principi contenuti nel Codice Etico, provvede a fornire ai Destinatari del Modello i principi di comportamento e specifiche attività di controllo da rispettare nell'esercizio delle attività "a rischio 231" individuate, con particolare riferimento alla gestione dei sistemi informativi. Le attività di controllo descritte sono demandate alla responsabilità primaria del management e del personale operativo e sono considerate parte integrante di ogni processo aziendale.

2. Principi di comportamento

I Destinatari del Modello, a qualsiasi titolo coinvolti nel processo di gestione e utilizzo dei sistemi informativi, sono tenuti ad osservare le modalità operative dettagliate dalla normativa interna della Società, le regole sancite dal presente protocollo, le previsioni di legge esistenti in materia nonché le norme comportamentali richiamate nel Codice Etico di cui la Società si è dotata.

3. Principi di controllo

Gestione degli accessi logici

- Ogni dipendente fornito di utenza logica ha a disposizione un PC desktop connesso alla rete aziendale tramite un indirizzo IP fisso;
- l'accesso ai Sistemi Informativi aziendali è consentito solo al personale autorizzato; Gli utenti definiti nominalmente e in gruppo hanno accesso alle cartelle e files definiti con il proprio responsabile;
- l'accesso al dominio di sistema (Active Directory) avviene tramite autenticazione univoca dell'utente;
- il riconoscimento dell'utente avviene attraverso username e password;
- ogni dipendente è dotato di indirizzo di posta elettronica nominativo ad esclusivo uso lavorativo; sono inoltre definiti indirizzi di posta elettronica per funzione cui hanno accesso più dipendenti;
- l'accesso alle cartelle di rete è profilato per funzione di appartenenza;
- l'accesso all'applicativo gestionale avviene tramite credenziali di accesso nominative e personali;
- le connessioni al sistema da remoto avvengono tramite canali di comunicazione sicuri e sono consentite solo al personale autorizzato; esistono diversi gestionali e le connessioni avvengono, in alcuni casi tramite ASP in https, in altri casi con una connessione client/server in intranet con credenziali nominative;
- è definita una procedura formale per la richiesta di creazione/disabilitazione di utenti o cambiamenti ai profili abilitativi;
- la comunicazione delle password di accesso all'applicativo gestionale avviene in modalità confidenziale ed è cura di ogni dipendente la custodia e non divulgazione;

- sono effettuate revisioni periodiche delle utenze attive al fine di garantire la corretta profilazione e concessione dei privilegi a sistema;
- sono implementate politiche di rinnovo periodico delle password del gestionale in linea a quanto richiesto dalla normativa sulla privacy;
- sono implementate politiche di rinnovo periodico delle password in automatico per l'Active Directory e Posta elettronica.

Gestione dei back up

- La Società dispone di un piano di backup periodico dei dati, file, programmi e sistemi operativi;
- giornalmente viene verificato il buon esito delle operazioni controllando appositi log generati in automatico dal software di backup;
- l'effettuazione di test di restore volti a verificare l'integrità dei supporti di backup e la conservazione dei back seguono quanto definito all'interno del progetto realizzato per l'aggiornamento della privacy nell'ambito della normativa vigente.

Gestione asset it

- Solo il Responsabile IT è autorizzato ad installare software.

Gestione della sicurezza di rete

- La rete interna è confinata e protetta da un firewall;
- server e client sono dotati di software antivirus aggiornati automaticamente;
- il server di posta Exchange è dotato di filtri antispamming, antiphishing e antivirus;(questi sistemi definiti UTM sono presenti sul firewall)
- le attività di Audit sulla sicurezza degli accessi e dei sistemi (es. Vulnerability Assessment) seguono quanto definito all'interno del progetto realizzato per l'aggiornamento della privacy nell'ambito della normativa vigente;
- l'accesso ai siti internet di enti pubblici o privati che richiedano credenziali di accesso (user-id, password e/o Smart Card) è consentito solo al personale autorizzato;
- viene mantiene costantemente aggiornato l'inventario dei siti di enti pubblici o privati acceduti dal personale che richiedano credenziali di accesso (user-id, password e/o Smart Card);
- l'accesso ad Internet è regolamentato a seconda delle effettive esigenze.

Accesso alla sala ced

- Gli accessi alla sala Ced sono stati definiti all'interno del progetto realizzato per l'aggiornamento della privacy nell'ambito della normativa vigente.

4. Flussi informativi verso l'Organismo di Vigilanza

Ad integrazione di quanto sopra e allo scopo di agevolare l'attività di vigilanza sull'operatività del Modello di Organizzazione, Gestione e Controllo adottato da Saronno Servizi ai sensi del D. Lgs. 231/2001, tutte le strutture aziendali sono tenute ad un obbligo di informativa verso l'Organismo di Vigilanza secondo le modalità descritte nel già menzionato Modello cui si rimanda.

In particolare le persone coinvolte nel processo sono tenute a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi eccezione comportamentale o qualsiasi evento inusuale, indicando le ragioni delle difformità.

Ogni modifica al presente documento deve essere effettuata in coordinamento all'Organismo di Vigilanza che ne valuterà l'adeguatezza e la coerenza rispetto al Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D. Lgs. 231/ 2001.