

**MODELLO DI ORGANIZZAZIONE, GESTIONE E
CONTROLLO
EX D.LGS. 231/2001**

**PARTE SPECIALE N. 2
REATI INFORMATICI**

PARTE SPECIALE N. 2 “REATI INFORMATICI”

1. LE FATTISPECIE PREVISTE DALL’ART. 24-BIS DEL D.LGS. 231/2001

Per il dettaglio dei reati presupposto previsti dall’art. 24-bis del D.Lgs. 231/2001 si richiama l’allegato 1 del Modello Organizzativo di Gestione e Controllo (catalogo dei reati presupposto ai sensi del D.Lgs. 231/2001).

2. LE ATTIVITÀ SENSIBILI

Si premette che l’Azienda esula dal perimetro applicativo della Nis 2 (D.Lgs. 138/2024) come da comunicazione ufficiale dell’Agenzia per la Cybersicurezza Nazionale nel 2025.

L’analisi dell’attività aziendale a valle della stesura delle interviste alle varie funzioni dell’Azienda, ha consentito di individuare le seguenti attività sensibili:

RI. 1 Privacy e tutela del dato

RI. 2 Sistema gestione della sicurezza informatica

RI 3 Utilizzo della dotazione informatica

In tale ambito rientrano:

- ☐ la prevenzione di quei delitti da cui scaturisce la responsabilità amministrativa/penale dell’ente, con particolare riferimento proprio ai delitti informatici o al trattamento illecito dei dati di cui all’art. 24 – bis del D.lgs. 231/2001;
- ☐ le attività operative compiute con l’ausilio di apparecchiature informatiche e/o sistemi informatici dai dipendenti e/o collaboratori di ACSI;
- ☐ le attività inerenti la gestione degli accessi alle risorse informatiche da parte degli utenti di ACSI e tali da garantire la protezione e il monitoraggio delle postazioni di lavoro ed il corretto utilizzo delle risorse, della posta elettronica e della sicurezza informatica, con particolare riguardo alla gestione di documenti elettronici con dati particolari o amministrativi;
- ☐ la trasmissione dei flussi informativi ai Comuni Soci, ad altri Enti Pubblici e alla Regione per la rendicontazione dei progetti, servizi, attività, interventi, sociali, socio-assistenziali e socio-sanitari integrati.

3. I PROTOCOLLI DI CONTROLLO

Politiche di sicurezza

L’Azienda ha adottato il Codice Etico, ove sono poste le regole comportamentali cui i dipendenti della Azienda e tutti coloro che contribuiscono allo svolgimento delle attività aziendali devono uniformarsi.

Tale Codice prevede che tutti gli utenti interni e quelli esterni autorizzati all’uso delle apparecchiature e dei sistemi informatici dell’Azienda debbano servirsi delle risorse informatiche aziendali nel rispetto delle disposizioni normative vigenti: sono espressi

il divieto di intrusione, accesso abusivo al Sistema Informatico e di danneggiamento di sistemi informatici altrui.

È inoltre affermato l'obbligo per tutti gli utenti di tutelare l'integrità delle apparecchiature e dei sistemi informatici interni, astenendosi da manipolazioni che ne possano modificare in qualsiasi modo le funzionalità.

Il Codice Etico è stato trasmesso telematicamente a tutti i dipendenti e viene aggiornato dal Consiglio di Amministrazione dell'Azienda.

La Azienda gestisce inoltre le apparecchiature informatiche in conformità a quanto stabilito dall'Autorità Garante per la tutela dei dati personali in tema di adeguate misure di sicurezza tecniche ed organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi in materia di sicurezza del trattamento dei dati previsti dal Regolamento UE 679/16.

Organizzazione della sicurezza per gli utenti interni

I profili utente dei dipendenti sono standard e prevedono le stesse abilitazioni: il profilo utente di ogni dipendente permette l'accesso alle risorse informatiche attraverso connessione protetta ed autenticazione personale.

Ogni profilo utente è utilizzato previo inserimento di credenziali univoche ed individuali (password). Ciascun dipendente può accedere solo alla propria area di competenza per adempiere ai compiti assegnati.

Le credenziali di autenticazione non utilizzate da più di tre mesi sono disattivate, salvo il rilascio di apposite autorizzazione per le sole esigenze di gestione tecnica.

Organizzazione della sicurezza per gli utenti esterni

L'Azienda non ha attivato profili per utenti esterni, eccezion fatta per i dipendenti espressamente autorizzati dall'Amministratore di Sistema dell'Azienda; l'accesso di eventuali ulteriori utenti, anche esterni, ai sistemi aziendali è espressamente autorizzato dall'Azienda.

Classificazione e controllo dei beni

Gli assets informatici dell'Azienda risultano tracciati.

I dati sottoposti a trattamenti manuali presenti su supporti non informatici sono raccolti in appositi archivi, di cui è responsabile il dipendente incaricato della gestione dei dati.

I documenti aziendali sono sottoposti a registrazione ed a classificazione e sono memorizzati in maniera tracciabile, al fine di garantirne l'autenticità e l'affidabilità.

L'Azienda ha definito la struttura organizzativa dei soggetti con attribuzioni ai sensi del Regolamento UE 679/16. Il Direttore Generale è stato individuato espressione del "Titolare del trattamento dei dati" ai sensi art. 4 comma 7 e art. 24 del Regolamento UE 679/16.

I Responsabili dei vari Servizi/Aree sono stati nominati Responsabili del trattamento dati dei propri settori ai sensi art. 4 comma 8 e art. 28 del Regolamento UE 679/16. Gli stessi hanno poi formalizzato le nomine ai Sub-Responsabili ai sensi art. 28 comma 4 del Regolamento UE 679/16. Tutti gli altri dipendenti sono stati nominati Incaricati Autorizzati ai sensi art. 28 comma 3 lett. b) e art. 29 del Regolamento UE 679/16.

Sicurezza fisica e ambientale

La protezione fisica delle attrezzature informatiche in dotazione è garantita dalle adeguate misure di sicurezza adottate nei locali degli uffici.

Gestione delle comunicazioni e dell'operatività

L'Azienda si avvale delle procedure di salvataggio automatizzato e conservato sul server, effettuato tramite sistemi di gestione che periodicamente effettuano una copia dei dati presenti sul server della sede e ne effettuano una copia su dispositivi che risiedono presso la Società di consulenza esterna informatica.

La protezione da software pericoloso è attuata attraverso il firewall, appositi software antivirus e antispam.

L'installazione e l'attivazione delle licenze software sono monitorate dalla Società di consulenza esterna, che monitora le rispettive scadenze.

L'Azienda si avvale dell'installazione di appositi software antivirus e antispam, aggiornati costantemente ed attivati dall'Azienda su tutti i firewall, mail di posta, intranet server e sui desktop dei pc.

Controllo degli accessi

In caso di risoluzione del rapporto di lavoro di un dipendente con l'Azienda, la stessa dispone la disabilitazione del profilo utente.

Gestione degli incidenti e dei problemi di sicurezza informatica

Malfunzionamenti o anomalie sul funzionamento dei sistemi e delle apparecchiature informatiche di Sede (ad es. server, rete, singoli software) sono gestiti dalla Società di consulenza esterna.

Audit

La verifica circa l'efficacia e l'efficienza della gestione della sicurezza informatica è affidata all'Amministratore di Sistema che annualmente stila una propria Relazione indirizzata al Titolare del Trattamento, e alla Società di consulenza esterna.

Risorse umane e sicurezza

L'Azienda ha comunicato a tutti dipendenti il contenuto del Codice Etico.

In caso di risoluzione del rapporto di lavoro di un dipendente, quest'ultimo ha l'obbligo di restituire tutte le apparecchiature ricevute.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei Sistemi Informativi

Sono installati unicamente software con apposita licenza d'uso ed è vietato l'utilizzo di software per i quali l'Azienda non abbia provveduto ad acquistare l'apposita licenza: in particolare, l'Azienda pone il divieto di duplicare, installare e/o detenere programmi ed ogni altro prodotto software senza esplicita autorizzazione e il divieto di utilizzare prodotti software per eseguire attività connesse a finalità personali dalle quali derivi direttamente o indirettamente un lucro per il lavoratore o un danno per l'Azienda.

Il download di software può essere effettuato solo per scopi professionali.

Gli interventi di manutenzione correttiva ed evolutiva sulla rete e sui sistemi di rete della Sede sono eseguiti dalla Società di consulenza esterna.

Le evoluzioni o personalizzazioni dei software installati sono gestite dalla Società di consulenza esterna.

Tutti i software e file scaricati legittimamente da internet o provenienti da fonti esterne all'Azienda sono controllati mediante software specifico di rilevazione virus prima che il file o software abbia contatto con altri programmi.

Tutte le componenti hardware sono registrate.

L'uso di risorse è monitorato e regolato dall'Amministratore di Sistema, alla quale spetta il compito di controllare i cambiamenti apportati ai sistemi ed alle strutture di elaborazione delle informazioni.

4. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Oltre agli obblighi informativi verso l'O.d.V. richiamati nella Parte Generale, saranno definiti specifici flussi di reporting di dati e/o informazioni relativi ai processi sensibili e strumentali individuati nella presente Parte Speciale, come sarà previsto nel documento denominato *“Flussi di reporting delle unità organizzative verso l'Organismo di Vigilanza per attività sensibile”*

Su base annuale, l'Amministratore di Sistema formalizza all'OdV apposita relazione scritta sullo stato dei sistemi informatici e dei sistemi informativi secondo i seguenti items:

- 1- Stato dei sistemi informatici e informativi dell'Azienda.
- 2- Eventuali elementi di vulnerabilità.
- 3- Stato del sistema di protezione da virus e attacchi informatici.
- 4- Previsione della business continuity plan.
- 5- Previsione del disaster recovery plan.
- 6- Sistema di log di sistema.
- 7- Sistema di backup dei dati aziendali.
- 8- Sistema di crittazione e cifratura per la tutela dei dati particolari e giudiziari.
- 9- Eventuali audit o penetration test effettuati.
- 10- Stato del server dell'Azienda
- 11- Manuale della conservazione digitale e Responsabile della conservazione digitale.