IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

PARTE SPECIALE

Gestione dei sistemi informativi

PSA VENICE

VECON S.p.A.

Porto Commerciale – Molo B
Porto Marghera (VE)

[ai sensi dell'art. 6, comma 3, del Decreto legislativo 8 giugno 2001, n. 231
"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"]

Aggiornato a Maggio 2024 – rev. 09

INDICE

FINALITA'

La presente Parte Speciale definisce le regole che tutti i soggetti aziendali (organi sociali, lavoratori e collaboratori della Società) coinvolti nelle attività sensibili elencate nel successivo paragrafo 2 dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Nello specifico, si intende:

- indicare i principi di comportamento e i presidi di controllo che i soggetti aziendali devono osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed alle altre strutture di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

In linea generale, tutti i soggetti aziendali, ciascuno per le aree di propria competenza, dovranno tenere comportamenti conformi a:

- Parte Generale del Modello;
- Codice Etico;
- corpo normativo e procedurale;
- sistema di deleghe e procure;
- ogni altro documento aziendale che regoli attività rientranti nell'ambito di applicazione del Decreto.

È espressamente vietato adottare comportamenti contrari a quanto previsto dalla normativa vigente e applicabile alla Società.

ATTIVITA' SENSIBILI

Le attività risultate rilevanti nel presente processo sono:

- gestione e protezione profili utente e processo di autenticazione
- gestione delle postazioni di lavoro
- gestione e protezione della rete aziendale
- gestione dei sistemi informativi

Gli strumenti informatici sono essenziali per il funzionamento dei processi operativi e di business, per soddisfare la costante esigenza di miglioramento, in termini di maggiore efficacia e di efficienza.
Si evidenzia che VECON ha implementato un sistema di controllo per la prevenzione dei reati di criminalità informatica che comprende una suite di macrosistemi tecnologici e un insieme di sistemi di gestione/controllo dell'area informatica.
In conformità alle direttive della casa madre, di recente compendiate in un piano pluriennale di sviluppo chiamato PSA Cyber Security Master Plan (CSMP), sono state altresì adottate procedure conformi al PSA Global Information Technology Security Standards (suite di standard di sicurezza definiti dalle normative ISO 27001 e ISO 27002).
Il sistema definisce:
1)i ruoli e le responsabilità del personale nell'ambito della protezione delle informazioni e delle risorse IT durante lo svolgimento del proprio lavoro;
2)la sicurezza degli asset IT secondo il seguente schema di divieti che il personale deve adottare

- accesso ai dati o alle applicazioni ai quali non si è autorizzati ad accedere
- utilizzo di un account o di password assegnati ad altri
- danneggiamento della rete e dei sistemi
- tentativo di eludere i sistemi di sicurezza
- tentativo di sfruttare o sondare eventuali falle di sicurezza nei sistemi informativi
- tentativo di lanciare vari attacchi in grado di ridurre le prestazioni o di bloccare i sistemi;

3)la Sicurezza dell'accesso in rete;
4)la sicurezza della posta elettronica;
5)la sicurezza dell'uso di Internet;
6)le segnalazioni degli incidenti di sicurezza informatica;
7)le sanzioni per la violazione delle norme di sicurezza IT.
VECON S.p.A. utilizza la piattaforma Oracle per la gestione globale degli approvvigionamenti, dei movimenti operativi/amministrativi/finanziari della società e rappresenta, contestualmente, uno dei massimi filtri di controllo e tracciabilità di ogni operazione funzionale e di business svolta in ambito societario.
Il personale appartenente alle diverse funzioni aziendali fa un intenso uso dello strumento informatico, quale utente interno, nell'ambito dei seguenti procedimenti:

a) gestione dei rapporti con i clienti
b) gestione dei rapporti con i fornitori e fatturazione dei servizi/prodotti forniti
c) amministrazione, contabilità e controllo di gestione
d) gestione dei pagamenti mediante piattaforme home banking

La figura degli addetti alla gestione dei sistemi informatici aziendali, svolgono le seguenti attività:

a) attivazione/gestione dei servizi informatici
b) attivazione/gestione delle infrastrutture tecnologiche di rete di VECON.

I REATI POTENZIALI

I reati che astrattamente potrebbero essere commessi nell'ambito del processo in questione sono:
- i reati informatici e di trattamento illecito dei dati di cui all'art. 24 bis D.Lgs. 231/2001
- i reati in materia di violazione del diritto d'autore di cui all'art. 24 novies D.Lgs. 231/2001

FIGURE AZIENDALI COINVOLTE

I successivi principi di comportamento e presidi di controllo si applicano a tutti i soggetti aziendali coinvolti nel processo e in particolare, ma non esclusivamente, a:
- Responsabile reparto Sistemi Informati Manager
- Personale che utilizza sistemi IT

PRINCIPI DI COMPORTAMENTO

I soggetti che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito delle attività sensibili devono:
- verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità nel sistema dei controlli informatici;
- valutare la corretta implementazione tecnica del sistema "deleghe e poteri" aziendale a livello di sistemi informativi ed abilitazioni utente riconducibile ad una corretta segregazione dei compiti;
- garantire, sui diversi applicativi aziendali, l'applicazione delle regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;
- monitorare il corretto utilizzo degli accessi (user-id, password) ai sistemi informativi aziendali e di terze parti;
- monitorare gli accessi tramite VPN;
- monitorare il corretto utilizzo degli accessi fisici ai sistemi informativi di dipendenti e terze parti;
- installare a tutti gli utenti esclusivamente software originali, debitamente autorizzati o licenziati;
- monitorare l'infrastruttura tecnologica al fine di garantirne la manutenzione e la sicurezza fisica;
- effettuare le attività di back-up e provvedere al corretto mantenimento dei file di log generati dai sistemi;
- garantire la manutenzione software e hardware dei sistemi e un processo di change management segregato.

Tutti i dipendenti devono:
- utilizzare gli strumenti informatici aziendali e assegnati nel rispetto delle procedure aziendali in vigore ed esclusivamente per l'espletamento della propria attività lavorativa;
- utilizzare la navigazione in Internet e la posta elettronica esclusivamente per le attività lavorative;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le password;
- custodire accuratamente le risorse informatiche aziendali o di terze parti (es. personal computer fissi o portatili) utilizzate per l'espletamento delle attività lavorative;
- rispettare le policy di sicurezza per l'accesso a sistemi o infrastrutture di parti terze.

È vietato:

- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di
▪ acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
▪ danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
▪ utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi.
- distruggere o alterare documenti informatici archiviati sulle directory di rete o sugli applicativi aziendali e, in particolare, i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- danneggiare, distruggere gli archivi o i supporti relativi all'esecuzione delle attività di back-up;
- utilizzare o installare programmi diversi da quelli autorizzati e privi di licenza;
- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- effettuare download illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;
- salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore;
- accedere ad aree riservate (quali server rooms, locali tecnici, etc.) senza idonea autorizzazione, temporanea o permanente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (antivirus, firewall, proxy server, etc.) della Società o di terze parti;
- lasciare il proprio personal computer o altri dispositivi di memorizzazione portatile incustoditi e senza protezione;
- rivelare a terzi le proprie credenziali di autenticazione (nome utente e password);
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- utilizzare in modo improprio gli strumenti di firma digitale eventualmente assegnati;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per la Società.

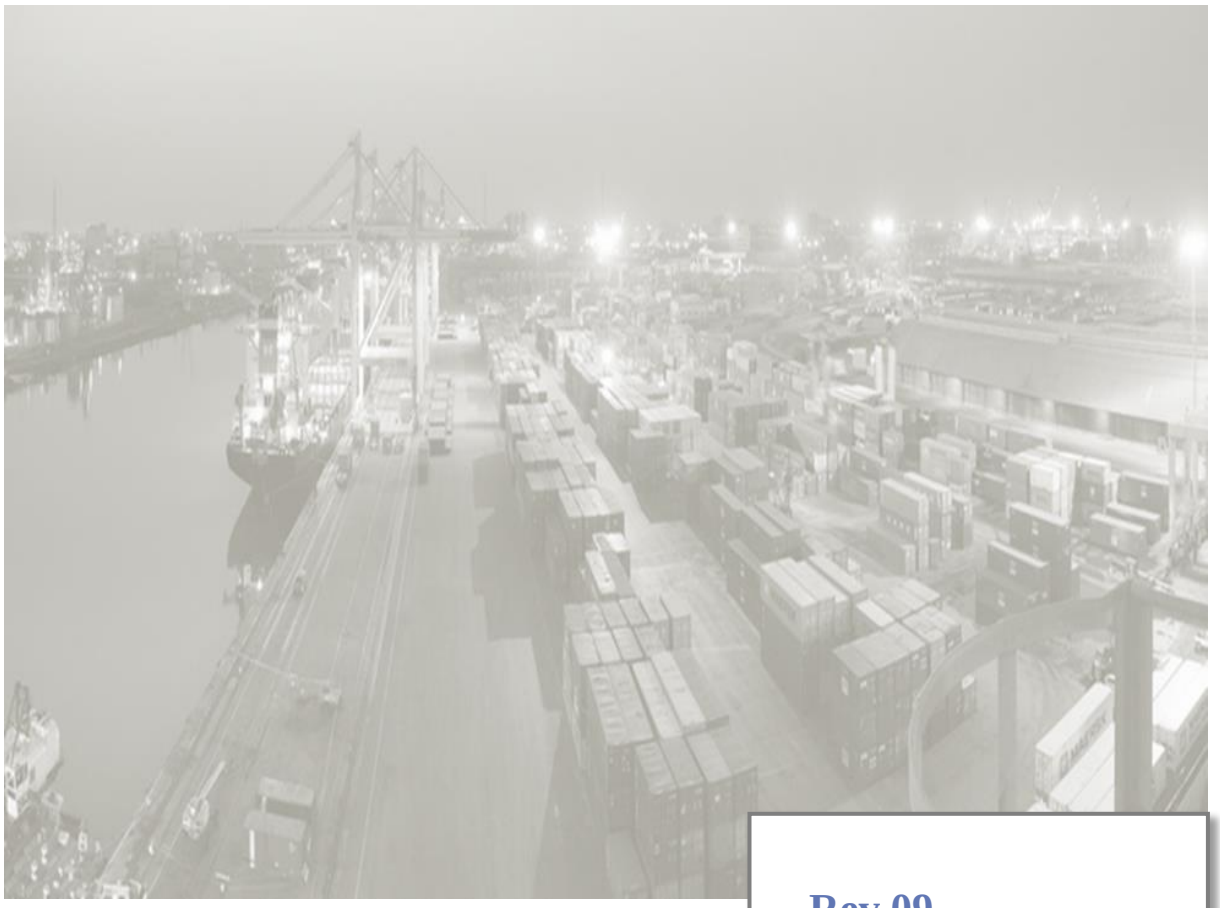
Procedura di controllo

Il sistema di controllo per la prevenzione dei reati di criminalità informatica deve basarsi su alcuni elementi di controllo:

- la separazione dei ruoli tra chi autorizza gli interventi di gestione sui sistemi informatici e chi realizza materialmente detti interventi;
- la tracciabilità degli accessi e delle attività svolte sui sistemi informatici;
- la raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio di consumazione reati informatici.

Flussi informativi nei confronti dell'Organismo di Vigilanza

Il Responsabile dei Sistemi Informativi trasmette annualmente l'elenco delle anomalie negli accessi informatici.



Rev.09
2024