Modello

231

STEELFORM SRL

SEDE LEGALE
Via Max Piccini, 16
33061 Rivignano-Teor (UD)
Tel. +390432822211
Fax. +390432822232
Web: www.steelformitalia.it
e-mail: info@steelformitalia.it

SEDI OPERATIVE
Via Max Piccini, 16 – 33061 Rivignano-Teor (UD)
Via Udine, 60 – 33061 Rivignano-Teor (UD)
Via Taglio, 11 – 33061 Rivignano-Teor (UD)
Via Taglio, 14 – 33061 Rivignano-Teor (UD)

Modello Organizzativo di Gestione e Controllo ex D. Lgs. 231/2001

Parte Speciale

PS-GESTIONE SISTEMI INFORMATICI

Tabella delle revisioni/aggiornamenti del presente documento		
REV.	**DATA**	**MOTIVO**

Emesso da:	Verificato da:	Approvato da:

PROTOCOLLO 231	CODICE DOCUMENTO	PS-IT
	TITOLO PROTOCOLLO	GESTIONE SISTEMI INFORMATICI
REFERENTE DEL PROCESSO	Resp. IT	
DESCRIZIONE SINTETICA DEL PROCESSO	Il processo comprende la selezione, inserimento, gestione e monitoraggio di tutti i sistemi informatici utilizzati in azienda. Il processo è complementare al sistema di gestione della protezione dei dati personali, in quanto le misure di mitigazione dei rischi implementate dall'organizzazione, oltre che essere finalizzate alla gestione dei dati personali, sono adatte anche a prevenire i rischi correlati ai reati informatici. L'utilizzo e la gestione di sistemi informatici sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi di gestione dei flussi informativi aziendali. Tra i sistemi informativi utilizzati dalla Società vi sono altresì hardware e software per l'espletamento di adempimenti verso la Pubblica Amministrazione che prevedono il ricorso a specifici programmi forniti dagli stessi Enti, ovvero la connessione diretta con gli stessi. L'azienda dispone di un responsabile IT (ITC manager) che cura tutti gli aspetti legati alla gestione dei sistemi informativi aziendali, nonché dispone dei privilegi di amministratore sulla rete aziendale.	

FAMIGLIE DI REATO COINVOLTE NEL PROCESSO
Delitti informatici e trattamento illecito dei dati (art. 24-bis, D. Lgs. 231/01)
Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies 1, D. Lgs. 231/01)
Delitti in materia di violazione del diritto d'autore (art. 25-novies, D. Lgs. 231/01)

FUNZIONI COINVOLTE
Amministratore Unico
Responsabile IT

PRINCIPI GENERALI APPLICABILI AL PROCESSO
Rispetto, da parte di tutti i Destinatari, dei principi stabiliti nel Codice Etico aziendale.
Divieto di porre in essere comportamenti che possano indurre qualsiasi soggetto a presentare dichiarazioni non vere.
Verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati.

Identificare le potenziali vulnerabilità nel sistema dei controlli IT.
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 risorse informatiche aziendali o di terze parti (es. personal computer fissi o portatili) utilizzate per l'espletamento delle attività lavorative.
Divieto di utilizzare i sistemi informativi a disposizione per attività non autorizzate nell'ambito dell'espletamento delle attività lavorative.
Divieto di porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali o di terze parti.
Divieto di intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche.
Divieto di salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore.
Prestare completa, trasparente ed immediata collaborazione all'Autorità Giudiziaria, fornendo dichiarazioni veritiere, complete, corrette e rappresentative dei fatti, e fornendo inoltre puntualmente ed esaustivamente la documentazione e le informazioni richieste.
Avvertire tempestivamente il proprio responsabile gerarchico e/o l'Organismo di Vigilanza di ogni minaccia, pressione, offerta o promessa di denaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da utilizzare in procedimenti penali.
Assicurarsi che le inserzioni e le informazioni inserite nel sito internet corrispondano a verità e alla realtà aziendale.
Verificare che nel sito non vengano inseriti marchi o segni distintivi o altri simboli simili o che richiamino aziende e/o prodotti di terzi.
Divieto di utilizzare termini denigratori, diffamatori, offensivi calunniosi o comunque non rispettosi nei confronti di terzi per descrivere o reclamizzare la propria azienda e i propri prodotti.
PROTEZIONE DEI DATI
Tutte le informazioni aziendali che risiedano su server, gestionali o pc devono essere sottoposti a regolare procedura di back up.
Verificare la sicurezza fisica e dei sistemi informativi aziendali e tutelare la sicurezza dei dati.

L'accesso ai luoghi fisici ove vengono archiviati i dati (locali in cui si trova il server) sono chiusi a chiave e l'accesso è consentito solo al personale autorizzato.
Divieto di manipolare fraudolentemente dati o informazioni presenti su supporto informatico, al fine di commettere illeciti.
Divieto di aggirare o tentare di eludere i meccanismi di sicurezza aziendali (Antivirus, Firewall, Proxy Server,) ecc.) di terze parti.
Divieto di produrre e trasmettere documenti in formato elettronico con dati falsi o alterati.
Divieto di 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.
GESTIONE CREDENZIALI E CRITERI DI ACCESSO
Valutare la corretta implementazione tecnica delle abilitazioni/profilazioni utente ai principali sistemi aziendali, verificandone la corrispondenza con le mansioni indicate dai Responsabili di ciascuna Funzione ed il rispetto del principio generale di segregazione dei compiti.
Identificare le persone dotate di accessi particolari (Internet, VPN, Siti esterni privati o pubblici, sistemi informativi esterni privati o pubblici) e credenziali specifiche.
Identificare i soggetti autorizzati ad effettuare i pagamenti con strumenti diversi dai contanti.
Individuare e/o programmare i sistemi di controllo degli accessi per i pagamenti telematici.
Divieto di introdursi abusivamente in un sistema informatico o telematico, contro la volontà del titolare del diritto di accesso.
Divieto di accedere a sistemi con accesso a credenziale attraverso le credenziali di altri colleghi.
Divieto di distribuire le proprie credenziali di accesso ai sistemi informatici ad altri.
Monitorare il corretto utilizzo degli accessi (user-id, password) ai sistemi informativi aziendali e di terze parti.
Divieto di entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato.
Garantire che non sia consentito l'accesso alle aree riservate (quali server rooms, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente e, in ogni caso, nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali.

Divieto di detenere, diffondere o utilizzare abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici.
Rispettare le policy di sicurezza concordate e definite con le terze parti per l'accesso a sistemi o infrastrutture di queste ultime.
Custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le password.
GESTIONE E UTILIZZO SOFTWARE E DEI PROGRAMMI
Divieto di installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata.
Monitorare le attività di fornitori terzi in materia di networking, gestione degli applicativi e gestione dei sistemi hardware.
Gestire la manutenzione software e hardware dei sistemi secondo le prassi esistenti.
Divieto di utilizzare dispositivi tecnici o strumenti software diversi di quelli specificamente autorizzati dalla Direzione.
Divieto di porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali o di terze parti.
Divieto di intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche.
Divieto di salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore.
Divieto di installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata.
Divieto di 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 l'azienda.
Divieto di accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente.
Deve essere previsto il costante monitoraggio sul corretto utilizzo delle licenze di software/banche dati.
Assicurare un sistema di blocco che non permetta al personale addetto alla registrazione delle fatture, di modificare gli ordini, gli archivi relativi al ricevimento merci, di accedere al menù dei pagamenti, fatture, ecc.

Predisporre un blocco al sistema per impedire l'emissione di ordini verso fornitori non qualificati.
Prevedere una verifica e/o blocco di sistema che impedisce di liquidare due vote la stessa fattura.

ACCESSO AI SISTEMI INFORMATICI DELLA PUBBLICA AMMINISTRAZIONE
In ogni caso, i documenti informatici dovranno essere creati, custoditi e inviati in modo da garantire la dovuta riservatezza (chi non è autorizzato non deve accedere al documento) e integrità (chi non è autorizzato non deve modificare il documento), attraverso l'adozione di idonee e preventive misure di sicurezza fisica o informatica a seconda delle modalità di trattamento.
Deve essere prevista l'autenticazione individuale degli utenti tramite log in e password o altro sistema di autenticazione sicura.
Devono essere disponibili liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti, nel caso in cui sia previsto un sistema di autorizzazione.
Deve essere previsto un sistema di autorizzazione (profili di utilizzo) per l'esecuzione di operazioni sui dati o per limitare la visibilità a un sottoinsieme dei dati stessi.

PROCEDURE DEL SISTEMA DI GESTIONE DI RIFERIMENTO	
SGQ P0001	Raccolta dei documenti, dati e registrazioni

CONTROLLI SPECIFICI DELL'ORGANISMO DI VIGILANZA
L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai processi sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al modello.
All'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonché viene garantito libero accesso a tutta la documentazione aziendale rilevante.
L'Organismo di Vigilanza può anche intervenire a seguito di segnalazioni ricevute.