SCM Group S.p.A.

IT Security Policy

SOMMARIO

1. PERIMETRO E OBIETTIVI

Questa policy fornisce una guida a tutto il personale di SCM Group ed eventuali terze parti sulle proprie responsabilità riguardo la gestione e utilizzo delle risorse informatiche IT e la responsabilità sulla loro proprietà. Inoltre, questa policy fornisce indicazioni sulla gestione delle identità, sulla sicurezza dei sistemi informatici e di rete, sui controlli delle strutture informatiche e il mantenimento del livello di sicurezza nel processo di evoluzione dei sistemi stessi. Questa policy ha tre obiettivi:

- **Riservatezza** – Protezione contro l'accesso non autorizzato, il furto o la divulgazione delle informazioni di SCM Group, accidentali o intenzionali.
- **Integrità** – Salvaguardia contro la modifica, la distruzione o la creazione non autorizzata di informazioni o comunicazioni elettroniche.
- **Disponibilità** – Protezione per garantire che il servizio non venga negato agli utenti autorizzati.

2. TERMINI E DEFINIZIONI

Tutti i termini e le definizioni sono contenuti nel corpo della policy stessa quando necessari.

3. PREMESSA

La presente IT Security policy si applica a tutti gli stakeholder di SCM Group nell'utilizzo dei dati, dei sistemi e delle infrastrutture informatiche di SCM Group.

La protezione delle informazioni prodotte da SCM Group e dei sistemi a supporto delle operazioni di SCM Group è responsabilità di tutti gli stakeholder di SCM Group. I sistemi a supporto dell'operatività di SCM Group e i dati elaborati, archiviati o trasmessi su di essi sono asset di vitale importanza per SCM Group. La politica di SCM Group è quella di adottare tutte le misure ragionevoli e appropriate necessarie per identificare e proteggere tutte le forme di informazioni non pubbliche originate o possedute dalla società o ad essa affidate da altri. Inoltre, devono essere prese tutte le misure ragionevoli e appropriate necessarie per proteggere i sistemi informatici che supportano le operazioni di SCM Group e i dati elaborati, archiviati o trasmessi su tali sistemi.

La protezione delle comunicazioni elettroniche a supporto delle operazioni di SCM Group è responsabilità di tutti gli stakeholder di SCM Group. Le comunicazioni elettroniche che utilizzano gli strumenti di comunicazione di SCM Group sono di proprietà di SCM Group. La policy di sicurezza informatica di SCM Group prevede l'adozione di tutte le misure ragionevoli e appropriate necessarie per proteggere i dati elaborati, archiviati o trasmessi elettronicamente a supporto delle operazioni di SCM Group. Il contenuto dei messaggi elettronici non deve essere monitorato a meno che non sia garantito da requisiti operativi, di manutenzione, di controllo, di sicurezza o investigativi.

Tutti gli stakeholder accedono ai sistemi che supportano le operazioni di SCM Group devono essere identificate, autenticate e autorizzate prima che venga concesso l'accesso. È responsabilità di tutti gli stakeholder di SCM Group garantire che questo avvenga secondo quanto definito nella seguente policy.

RIFERIMENTI

Policy Sponsor:	Comitato per la Sicurezza IT
Data efficacia:	Gennaio 2023
Versione numero:	1.0

REVISIONE DELLA POLICY E PROCESSO DI AGGIORNAMENTO

Il Comitato per la sicurezza IT deve rivedere annualmente l'IT Security policy di SCM Group per verificare potenziali modifiche e pubblicherà gli aggiornamenti approvati.

4. ORGANIZZAZIONE INTERNA DELLA SICUREZZA IT

RUOLI

Il Comitato per la sicurezza IT ha la responsabilità del programma globale di sicurezza e conformità ed è composto dal Direttore dei Sistemi (group information technology director) e dal responsabile della sicurezza IT (IT Infrastructure & Security Manager). Esso è governato dal Comitato di Direzione Aziendale i cui membri sono il CEO, general manager, group human resources and organization director, group chief financial officer, group information technology director, group communications director ed i vari Direttori di divisione.

Il team *IT Infrastructure & Security* ha la responsabilità globale per l'implementazione e il supporto continuo della sicurezza e del monitoraggio degli eventi, della gestione delle patch, della risposta agli incidenti e del provisioning degli utenti. Questo gruppo lavora a stretto contatto con il resto dell'organizzazione IT per eseguire la parte operativa.

RESPONSABILITÀ PER L'APPLICAZIONE DELLA POLICY

Manager e Direttori sono responsabili di:

- Comunicare e garantire il rispetto di questa policy e supportare le linee guida.
- Fornire indicazioni e decisioni in merito alla concessione e alla rimozione dell'accesso alle informazioni e ai sistemi di SCM Group.

Tutti gli stakeholder di SCM Group (ovvero dipendenti, fornitori di servizi, fornitori, appaltatori, consulenti, partner commerciali, di canale e di joint venture, consociate e affiliate) che generano, sono in possesso di, controllano informazioni o utilizzano apparecchiature informatiche coperte dalla presente policy sono responsabili della loro tutela in conformità con questa policy e delle linee guida a supporto.

5. ASSET MANAGEMENT

CONSEGNA E RESTITUZIONE ASSET

Al momento dell'assunzione di un dipendente che necessiti di un dispositivo elettronico (asset) che accede a dati aziendali trattati dal Gruppo SCM, il reparto IT aziendale assegna l'asset al dipendente, registrandone l'avvenuta consegna oltre ai dati identificativi del medesimo.

Allo stesso modo, al momento della cessazione del rapporto lavorativo, il dipendente che ha avuto l'asset, dovrà restituirlo, previa verifica e rilascio di dichiarazione di assenza nell'asset di dati personali ancorché involontariamente memorizzati benché vietato, sollevando l'azienda da eventuali responsabilità in caso di trattamento accidentale degli stessi. Il reparto IT registrerà l'avvenuta riconsegna e verificherà lo stato di funzionamento e conservazione dell'asset.

RESPOSABILITA' DEGLI ASSET

La direzione aziendale è responsabile della sicurezza dei dispositivi di SCM Group, tuttavia, questa responsabilità è ulteriormente delegata a dirigenti, responsabili, dipendenti e contractor a cui viene affidata la custodia di tali sistemi.

FURTO E SMARRIMENTO ASSET

In caso di furto o smarrimento di uno strumento di lavoro informativo aziendale il lavoratore/collaboratore a cui lo stesso era stato consegnato è tenuto a comunicare tempestivamente al reparto IT l'accaduto in modo che quest'ultimo possa, nel limite delle sue possibilità, bloccare qualsiasi accesso alle informazioni contenute in esso. Il dipendente deve inoltre in caso di furto, fare immediata denuncia alle autorità competenti.

Analoga segnalazione deve essere fatta dal lavoratore/collaboratore in caso di furto o smarrimento di dati su qualunque supporto (ad es. nel caso di furto e/o perdita di dischi USB esterni o chiavette USB di cui sia stato previamente autorizzato l'utilizzo; perdita di documento cartacei ecc.)

PROPRIETÀ DEL SOFTWARE SVILUPPATO PER SCM GROUP

Tutto il software per computer sviluppato da dipendenti, personale a contratto o fornitori per conto di SCM Group è di proprietà di SCM Group e non può essere distribuito al di fuori di SCM Group senza specifica autorizzazione. Le risorse informatiche in fase di sviluppo devono essere considerate di proprietà di SCM Group e devono essere protette.

RISPETTO DEGLI ACCORDI DI LICENZA/COPYRIGHT

Tutti gli sviluppatori devono rispettare gli accordi di licenza dei software di terze parti e delle leggi sul copyright. I prodotti software di terza parti possono essere distribuiti internamente solo in conformità con i rispettivi accordi di licenza.

USI CONSENTITI

SCM Group fornisce sistemi, servizi e strutture per condurre le attività aziendali. Tutti i dipendenti sono tenuti a rispettare i valori che rappresentano SCM Group nel loro utilizzo.

L'uso inappropriato, non etico o abusivo delle strutture o dei sistemi di SCM Group, da parte di qualsiasi utente, non sarà tollerato e sarà segnalato ad HR e Responsabili per valutare eventuali azioni disciplinari.

Esempi di uso inappropriato da parte dei dipendenti includono, ma non sono limitati a:

- Download o installazione di software commerciale in violazione dei relativi accordi di licenza
- Utilizzo di qualsiasi software o file elettronico scaricato da Internet senza scansione antivirus per il rilevamento di possibili minacce, la scansione antivirus viene eseguita automaticamente sulle apparecchiature configurate come da standard di SCM Group.
- Rimozione o compromissione di qualsiasi componente standard di sicurezza aziendale (es. Antivirus, etc).
- Interferire intenzionalmente con il normale funzionamento di qualsiasi infrastruttura di comunicazione (internet, LAN, etc).
- Utilizzare i sistemi di SCM Group per sostenere convinzioni politiche o religiose
- Invio di messaggi offensivi, calunniosi o dannosi per l'azienda o per i dipendenti di SCM Group.
- Accesso o download di materiale pornografico
- Utilizzo eccessivo di Internet per uso personale (Es. Streaming Video, etc).
- Svolgere attività illegali, incluso il gioco d'azzardo

STRUMENTI PERSONALI AD USO LAVORATIVO

È vietato utilizzare strumenti personali (a titolo esemplificativo: PC, tablet e smartphone) per trattare dati aziendali. Nel caso in cui tale utilizzo dovesse rendersi necessario, dovrà essere fatta richiesta scritta al Responsabile/Amministratore di sistema che valuterà caso per caso la reale necessità e suggerirà misure tecniche da adottare su tali dispositivi autorizzati. In ogni caso, i dati – specificatamente individuati – dovranno permanere su tali dispositivi personali per un tempo determinato e, comunque, non superiore al tempo necessario per il loro utilizzo.

A ciascun dipendente è assegnata una postazione di lavoro, attraverso la quale potranno essere svolte tutte le attività lavorative. È tuttavia possibile utilizzare anche altre postazioni in caso di necessità, accedendo con le credenziali di autenticazione assegnate.

È vietato salvare sul PC aziendale documenti personali o comunque contenenti dati riferibili a parenti, amici o conoscenti.

Nel caso di accesso da remoto ai dati contenuti nei sistemi, si deve prestare la massima attenzione affinché non siano salvate copie sui PC personali che dovranno, in ogni caso, essere cancellati ed eliminati anche dal “cestino”. Inoltre, i dispositivi elettronici che accedono devono necessariamente essere dotati di sistemi di protezione (quali ad esempio password di accesso, antivirus,) attivi ed aggiornati, per tutta la durata della connessione.

6. SICUREZZA FISICA E AMBIENTALE

6.1 AREE SICURE

STRUTTURE INFORMATICHE

CONTROLLO DELL'ACCESSO ALLE STRUTTURE INFORMATICHE

L'accesso alle strutture dedicate alle elaborazioni informatiche (ad es. data center e sale server) deve essere fisicamente limitato. Le autorizzazioni di accesso alle strutture informatiche devono essere concesse a coloro che hanno legittime responsabilità aziendali all'interno della struttura e che hanno una frequente necessità di accesso alle suddette aree. Il relativo responsabile IT deve approvare tutte le richieste di accesso. Ove possibile, devono essere implementati sistemi elettronici di controllo degli accessi per impedire l'accesso non autorizzato. Il sistema deve registrare tutte le entrate e deve essere in grado di produrre un report se richiesto.

Le tessere o i badge di accesso del personale autorizzato che non ha più necessità di accesso devono essere ritirati prima della sua uscita dall’azienda.

CONTROLLO VISITATORI

Il personale che non richiede l'accesso continuo alle strutture informatiche ("visitatori") deve essere scortato da una persona autorizzata.

PIANIFICAZIONE DELLE ATTIVITÀ DI MANUTENZIONE

Le attività di manutenzione devono essere programmate solo previa conoscenza e consenso del responsabile IT della specifica struttura informatica.

6.2 SICUREZZA DELL'ATTREZZATURA

SICUREZZA DELLE APPARECCHIATURE di TELECOMUNICAZIONE, NETWORK E SERVER

Tutte le apparecchiature per telecomunicazioni, reti e server devono trovarsi in una struttura protetta. Se possibile, deve essere ospitato in una sala server dedicata o in un data center. Se ciò non è possibile, tali apparecchiature devono essere custodite in locali chiusi a chiave. Non devono trovarsi nelle aree degli uffici.

MOVIMENTAZIONE DELLE ATTREZZATURE FUORI SITO

La rimozione non autorizzata dei computer aziendali sarà considerata furto. I computer non portatili possono essere rimossi dai locali aziendali solo in presenza di apposita autorizzazione da parte della direzione della sede e dal responsabile IT per quella sede.

- **Sicurezza dei dispositivi portatili:** i controlli di accesso logico devono essere implementati in modo che gli utenti non autorizzati non possano accedere alle informazioni memorizzate sul dispositivo. I dispositivi portatili non devono essere lasciati incustoditi o non protetti
- **Uso della crittografia:** la crittografia dei file o dei dischi deve essere utilizzata sui computer portatili per proteggere le informazioni riservate o sensibili di SCM Group in caso di furto delle apparecchiature.

7. INSTALLAZIONE, CONFIGURAZIONE E AGGIORNAMENTO DEI SISTEMI INFORMATICI

7.1 PROCEDURE OPERATIVE E RESPONSABILITA'

ACCETTAZIONE DEL SOFTWARE

Le caratteristiche di sicurezza del sistema devono essere esaminate con il proprietario o vendor del sistema prima dell'installazione e dell'utilizzo dello stesso. Prima dell'effettivo utilizzo, l'amministratore di sistema deve effettuare tutti i controlli di sicurezza. L'accesso degli utenti per scopi di produzione non deve essere consentito fino a quando le impostazioni relative alla sicurezza non saranno completamente operative e funzionanti.

GESTIONE DEGLI AGGIORNAMENTI DELLA CONFIGURAZIONE

UTILIZZO DI PROCEDURE FORMALI PER IL CONTROLLO DELLE MODIFICHE

Tutti i sistemi utilizzati per elaborazioni in produzione di SCM Group devono utilizzare la procedura *"4SCM - Procedura Change Management"* per disciplinare le attività necessarie per gestire correttamente il ciclo di vita del software.

Gli aggiornamenti dei programmi non devono essere scaricati da Internet, da fonti non verificate, direttamente su un server di produzione. Tutto il software scaricato deve essere scansionato alla ricerca di virus, esaminato per verificarne l'autenticità e testato accuratamente prima di essere messo in produzione (gli aggiornamenti di fornitori attendibili, come le definizioni dei virus e gli aggiornamenti delle firme, sono esentati da questo requisito).

SEGREGAZIONE DEI COMPITI NELL'UTILIZZO, SVILUPPO E AMMINISTRAZIONE DEL SISTEMA

La gestione o l'esecuzione di determinati compiti o aree di responsabilità devono essere separate nella misura in cui il rischio di modifica non autorizzata o uso improprio di dati/servizi è accettabile.

Funzioni critiche da segregare: le seguenti funzioni non devono essere svolte dagli stessi dipendenti in un ambiente di produzione:

- Utilizzo del sistema aziendale: un utente tipico che svolge normali operazioni aziendali
- Immissione dati: un utente dedicato all'immissione di dati massiva
- Operazioni informatiche: un utente tecnico che gestisce le attività operative quotidiane e può avere un accesso elevato al sistema
- Gestione della rete: un utente tecnico che gestisce i dispositivi di rete e potrebbe avere un accesso elevato ai dispositivi di rete
- Amministrazione di sistema: utente tecnico che installa e gestisce i sistemi operativi e dispone di un accesso elevato al sistema
- Manutenzione del sistema: un utente tecnico responsabile della manutenzione dell'hardware e che può avere accesso elevato al sistema
- Gestione delle modifiche: un utente tecnico responsabile della migrazione delle modifiche alla produzione e che può avere un accesso elevato al sistema

In generale, le persone con i diritti di accesso per implementare o migrare le modifiche nei sistemi di produzione dovrebbero essere separate dalle persone con responsabilità di sviluppo e utilizzo dei sistemi.

7.2 GESTIONE DELL'EROGAZIONE DI SERVIZI DI TERZE PARTI

AMBIENTI HOSTED

I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati di SCM Group garantendo che solo gli autorizzati abbiano accesso all'ambiente di SCM Group; garantendo che la registrazione e gli audit siano abilitati e univoci per l'ambiente di SCM Group e coerenti con tutti i requisiti normativi o di settore pertinenti. Devono inoltre consentire di fornire tempestive indagini forensi in caso di compromissione dell'ambiente o dei dati di SCM Group o di qualsiasi altra entità.

L'utilizzo delle risorse deve essere monitorato e si devono fare proiezioni sui requisiti di capacità futuri per garantire il funzionamento e le prestazioni richieste del sistema.

7.3 PROTEZIONE CONTRO SOFWTARE/CODICE DANNOSO

SOFTWARE DI PROTEZIONE DA VIRUS

Per rilevare tempestivamente e prevenire la diffusione di virus informatici, tutte le workstation, i server, i computer portatili, i laptop e i notebook di SCM Group devono essere configurati per caricare ed eseguire automaticamente il software di rilevamento dei virus, ove applicabile. Sui sistemi verranno installati solo prodotti di protezione antivirus standard e approvati dal management ottenuti da fornitori autorizzati.

CREAZIONE O INTRODUZIONE DI SOFTWARE DANNOSO

Gli utenti non devono creare né introdurre software dannoso su alcun sistema di SCM Group.

7.4 BACKUP

I dati informatici devono essere sempre salvati in aree dei sistemi aziendali che sono sottoposte a backup. Qualora non si conoscano tali aree nel sistema informativo, occorre rivolgersi al reparto IT aziendale o all'Amministratore di Sistema.

Tutti i sistemi utilizzati per elaborazioni in produzione di SCM Group devono utilizzare la procedura "*3SCM - Procedura Backup*" dove sono descritti i processi e le modalità adottati da SCM Group S.p.A. per la realizzazione delle attività di backup e di restore dei sistemi.

7.5 GESTIONE SICUREZZA DELLA RETE

RISERVATEZZA DEGLI INDIRIZZI DI RETE

Le informazioni relative agli indirizzi interni, alle configurazioni e ai relativi design delle reti e dei sistemi di SCM Group devono essere protette al fine di mantenerne la riservatezza e la conseguente integrità.

BLOCCO DEI SERVIZI DI RETE NON ESSENZIALI

Tutti i servizi di rete o di sistema non essenziali devono essere bloccati e rimossi dagli ambienti di produzione.

7.6 SCAMBIO DI INFORMAZIONI

UTILIZZO POSTA ELETTRONICA

Al dipendente possono essere assegnati uno o più indirizzi e-mail. Questi devono essere tutti utilizzati esclusivamente per finalità lavorative, dal momento che – in caso di necessità – la Società (proprietaria del dominio e, comunque, titolare del trattamento) potrà accedervi, nel rispetto dei requisiti di legge, anche in assenza del dipendente o al termine del rapporto lavorativo.

L'utilizzo della posta elettronica deve avvenire nel rispetto del presente regolamento e dei principi e regole che seguono:

a) Le caselle di posta elettronica fornite dall'Azienda sono messe a disposizione dei dipendenti per usi esclusivamente lavorativi e sono per questo da considerarsi, a tutti gli effetti beni immateriali dell'azienda e strumenti di lavoro anche ai sensi dell'art. 4 della l. 300/1970.

b) È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti web o server FTP non conosciuti).

c) È necessario porre la dovuta attenzione al contenuto delle mail in uscita in quanto, mediante le stesse, l'Utente rappresenta la Società nei confronti dei destinatari.

d) È necessario mantenere la casella di posta elettronica in ordine, cancellando documenti inutili ed allegati ingombranti;

e) È necessario procedere all'archiviazione dei documenti ricevuti e delle informazioni contenute nelle mail secondo le regole aziendali.

f) È consentito accedere a caselle di posta elettronica personali, esclusivamente tramite browser (ad esempio Google Chrome, Microsoft Edge) senza salvare documenti o file di qualsivoglia natura sul sistema informativo aziendale e durante le pause.

g) È vietato utilizzare la casella elettronica assegnata: (i) per l'invio di messaggi personali; (ii) per l'invio di messaggi ed estranei al rapporto di lavoro o alle relazioni lavorative tra colleghi; (iii) per inviare e scaricare allegati contenenti video/brani musicali non funzionali all'attività lavorativa; (iv) per la partecipazione a dibattiti, forum, mailing list; (v) per ogni altra finalità non connessa alla prestazione lavorativa.

h) È vietato aprire i file attachments di posta elettronica qualora il mittente sia sconosciuto o sia dubbia l'attinenza della comunicazione all'attività lavorativa.

i) È vietato l'utilizzo di software di posta elettronica (ad esempio Outlook, etc) ed il transito di qualsiasi file personale sulle mail aziendali e sugli strumenti di lavoro informatici ovvero sul sistema informativo aziendale in genere nonché qualunque transito di mail o dati aziendali su posta personale (è vietato pertanto, a titolo esemplificativo e non esaustivo, inviare o scaricare allegati, inoltrare – singolarmente o automaticamente - mail lavorative a indirizzi privati e viceversa ecc.). Nei casi di comprovata emergenza, sarà possibile utilizzare indirizzi di posta elettronica personali anche durante l'orario di lavoro avendo cura di comunicare la circostanza al Responsabile/Amministratore di sistema.

j) In caso di assenza prolungata l'utilizzatore della casella di posta elettronica aziendale dovrà impostare direttamente un avviso di risposta automatica che avvisi della sua irreperibilità e, se del caso, indichi altro indirizzo alternativo a cui inviare le mail.

Le informazioni relative all'accesso alle varie caselle aziendali, quali ad esempio la localizzazione dell'indirizzo IP dell'utente che accede al servizio di posta elettronica, nonché la data e l'ora di accesso, sono registrate per ragioni di sicurezza del sistema informatico e dei dati ivi trattati. Le suddette informazioni possono essere consultate dall'Amministratore di Sistema. I dati (intestazione e corpo dell'e-mail) possono essere presenti anche in copie di backup gestite direttamente dal fornitore del servizio di posta elettronica. Il fornitore garantisce la compliance del proprio sistema di posta elettronica ai requisiti normativi europee, in particolare si è optato per la funzione di conservazione delle informazioni in ambito del territorio della UE.

Alcuni indirizzi di posta elettronica, in particolare quelli non nominativi, potranno essere condivisi tra più soggetti. In tal caso ciascun utente deve attenersi scrupolosamente alle regole stabilite dalla presente procedura.

In caso di necessità, ad esempio per assenza temporanea - anche non programmata - di un dipendente/consulente qualora lo stesso non abbia attivato la funzionalità di risposta automatica e previa richiesta in forma scritta di un responsabile dell'Ufficio e con l'autorizzazione dalla Direzione e previa, altresì, comunicazione all'utente interessato, la Società per il tramite del Responsabile/Amministratore di sistema, potrà attivare tale funzionalità ed il reindirizzamento delle mail ad altro indirizzo mail. In questo caso si procederà alla cancellazione della password ed all'inserimento di una nuova. Il cambiamento della password ad opera del Responsabile/Amministratore di sistema è garanzia, per l'utente, che è stato effettuato da terzi un accesso autorizzato.

L'Azienda potrà accedere alla e-mail aziendale in caso di assenza del dipendente oppure alla conclusione del rapporto di lavoro, qualora si verifichino circostanze tali da rendere ciò necessario per la salvaguardia degli interessi aziendali (a titolo esemplificativo: in caso di urgenza che richieda di garantire una continuità operativa; per comprovate esigenze organizzative e produttive; per la sicurezza del lavoro e per la tutela del patrimonio aziendale, compreso quello informatico; per verificare l'integrità e la sicurezza dei sistemi; per accertare accessi abusivi, singoli o reiterati, al sistema informatico aziendale, ai dati e ai programmi; per violazione di materiale oggetto dei diritti di proprietà intellettuale dell'Azienda; in caso di serio sospetto di commissione di possibili illeciti, anche penali/amministrativi, a danno della Società o di soggetti terzi).

L'accesso alla casella di posta elettronica avverrà nel rispetto dei principi previsti dalla legge, comunque, secondo: il principio di proporzionalità (l'accesso ed il controllo avverrà per il tempo indispensabile per il

perseguimento delle finalità di cui sopra); il principio di trasparenza (il presente Regolamento ha infatti l'obiettivo di informare i dipendenti sui diritti e i doveri delle parti); il principio di pertinenza e non eccedenza (saranno utilizzate modalità che garantiscono la sicurezza e riservatezza per l'interessato, e il controllo non avrà carattere costante ed indiscriminato).

Alla cessazione del rapporto di lavoro l'account di posta aziendale assegnato al lavoratore verrà inibito l'accesso il giorno stesso e disattivato entro 15 giorni lavorativi.

Dopo la cessazione del rapporto di lavoro/collaborazione il contenuto della posta elettronica ed i relativi dati saranno conservati per un periodo di 6 mesi. Per i messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale la conservazione avverrà nel rispetto dei termini previsti dalla legge. Per tutelare i propri diritti in giudizio in caso di contenziosi o precontenziosi in atto la Società potrà conservare messaggi di posta elettronica per un periodo superiore a quelli sopra indicati e fino alla persistenza del suddetto legittimo interesse.

MODALITÀ TRASFERIMENTO DI DOCUMENTI AZIENDALI

È assolutamente vietato l'utilizzo di dispositivi rimovibili (a titolo esemplificativo, dischi USB esterni o chiavette USB) o anche spazi cloud non forniti dall'azienda in cui riversare in chiaro, anche solo temporaneamente, dati aziendali. Qualora, eccezionalmente, vengano utilizzati tali dispositivi il dipendente sarà considerato, a tutti gli effetti, custode degli stessi e dei dati ivi contenuti e ne risponderà di conseguenza anche dal punto di vista disciplinare.

Eventuali documenti e/o informazioni protetti, rispetto ai quali la Società risulta vincolato da specifici accordi (cc.dd. NDA, Non-Disclosure Agreement) non possono essere in alcun caso salvati su dispositivi mobili, tranne che ciò non sia espressamente autorizzato per iscritto dal proprio responsabile. Il Reparto IT indicherà le modalità di protezione del dato

7.7 MONITORAGGIO

Tutti i sistemi che elaborano, trasmettono o memorizzano le informazioni di SCM Group devono generare LOG. Devono essere implementate procedure per monitorare l'utilizzo del sistema su base regolare per garantire che gli utenti eseguano solo processi che sono stati loro esplicitamente autorizzati. La registrazione deve avere la forma di una registrazione cronologica delle attività che consenta la ricostruzione, la revisione e l'esame di qualsiasi sequenza scelta di attività.

LOGGING

ATTIVITÀ DA LOGGARE

Le attività da registrare devono includere, a titolo esemplificativo ma non esaustivo, gli attributi rilevanti (utente, data/ora, risorse, ecc.) di quanto segue:

- Attività eseguite
- Connessioni negate e tentativi rifiutati
- Successi e fallimenti di accesso
- Messaggi di errore e avvisi
- Attività di creazione e modifica degli account
- Assegnazione e utilizzo di account con capacità di accesso privilegiato
- Altre attività di amministrazione della sicurezza IT

UTILIZZO DI STRUMENTI PER RACCOLTA LOG

I Log devono essere inoltrati a un sistema di registrazione centrale (SIEM) per garantire l'integrità dei dati e facilitare il monitoraggio e gli avvisi. I log degli amministratori di sistema (AdS) devono essere mantenuti e non modificabili come richiesto dai titolari del trattamento effettuato con strumenti elettronici in relazione all'attribuzione delle funzioni di amministratore di sistema nel 2008 da parte del Garante per la protezione dei dati personali (D. lgs.196/2003).

REQUISITI MINIMI DI CONSERVAZIONE

I Log devono essere conservati per **un anno**.

PROTEZIONE DEI DATI DI LOG

I Log devono essere trattati come dati riservati di SCM Group e non possono essere modificati e cancellati da nessuno durante il periodo di conservazione.

SECURITY MONITORING MANAGEMENT

SCOPO DEL MONITORAGGIO

I sistemi e le reti critici e le attività svolte devono essere monitorati per garantire la conformità a tutte le politiche e linee guida sulla sicurezza IT.

UTILIZZO DI STRUMENTI PER RACCOLTA LOG

Gli strumenti automatizzati devono essere utilizzati su base continuativa per facilitare la revisione dei dati di Log (ad esempio firewall, Navigazione Internet, ecc.)

VERIFICA PERIODICA DELL'INTEGRITÀ DEI FIREWALL

L'integrità di tutti i sistemi firewall deve essere verificata in tempo reale utilizzando i metodi e le tecniche più recenti.

MONITORAGGIO UTILIZZO DEI SISTEMI

Devono essere stabilite procedure per il monitoraggio dell'uso del sistema per garantire che gli utenti eseguano solo processi che sono stati esplicitamente autorizzati. Il livello di monitoraggio richiesto per i singoli sistemi deve essere determinato in base alla sensibilità dei dati gestiti dal sistema. L'implementazione delle policy e delle linee guida relative alla sicurezza all'interno dell'ambiente distribuito deve essere monitorata a livello centrale. Le aree da considerare sono:

- Tentativi e fallimenti di accesso al sistema operativo e alle applicazioni
- Monitoraggio delle transazioni critiche selezionate
- L'utilizzo di risorse aziendali
- Attività del firewall
- Attività di amministrazione della sicurezza IT
- Pagine WWW visitate
- Sessioni FTP (dove consentito)
- Sessioni SSH
- Attività Sudo
- Accesso remoto da parte dei fornitori per manutenzione o diagnostica
- Accessi da remoto tramite VPN

MONITORAGGIO DI SICUREZZA REAL TIME

I sistemi di rilevamento delle intrusioni devono essere utilizzati per le connessioni Internet in entrata per rilevare i tentativi di attacco eseguendo l'analisi in tempo reale del traffico di rete. Lo stesso rilevamento è richiesto anche sulle connessioni di terze parti.

DIRITTO DI MONITORAGGIO E CONTROLLO

Gli utenti non devono avere alcuna aspettativa di privacy quando utilizzano i sistemi di comunicazione elettronica di SCM Group. In qualsiasi momento e senza preavviso, la direzione di SCM Group si riserva il diritto di esaminare le informazioni memorizzate sui sistemi di SCM Group (ad esempio messaggi di posta elettronica, elenchi di file personali) e può anche divulgare tali dati alle forze dell'ordine.

La politica di SCM Group NON prevede il monitoraggio dei messaggi elettronici a meno che non sia garantito da requisiti operativi, di manutenzione, audit, sicurezza o investigativi. Salvo specifica autorizzazione della direzione, è vietata l'intercettazione o la divulgazione di comunicazioni elettroniche.

FALSA IDENTITÀ E ANONIMATO

Gli utenti di SCM Group non devono, direttamente o implicitamente, utilizzare una falsa identità (il nome o l'identificazione elettronica di un altro). Un utente di SCM Group può utilizzare uno pseudonimo (un nome alternativo o un'identificazione elettronica per se stesso) per motivi di privacy o per altri motivi, a condizione che lo pseudonimo non costituisca chiaramente una falsa identità.

8. CONTROLLO DEGLI ACCESSI

8.1 REQUISITI AZIENDALI PER IL CONTROLLO DEGLI ACCESSI

PRINCIPIO “NEED-TO-KNOW“

Per ridurre il rischio di compromissione o impatto operativo negativo, l'accesso alle informazioni di SCM Group si basa sul principio "Need-to-Know". L'accesso dovrebbe essere limitato alle informazioni di cui una persona ha bisogno per adempiere alle responsabilità assegnate.

ACCESSO DA RETI ESTERNE

Tutti i sistemi e applicazioni devono implementare ove possibile l'autenticazione forte (MFA) e la crittografia per tutti gli accessi non pubblici da una rete esterna, incluso Internet. Qualsiasi sistema o applicazione esposta a Internet che ospita o consente l'accesso alle informazioni di SCM Group deve eseguire un sistema operativo protetto in modo appropriato.

DIRITTO DI SCM GROUP ALLA REVISIONE DEI CONTROLLI DI SICUREZZA IT

SCM Group, a sua discrezione, deve avere il diritto di rivedere i controlli di sicurezza di una terza parte per determinare se sono adeguati a proteggere le risorse creative di SCM Group e può, a sua discrezione, migliorare direttamente tali controlli di sicurezza per prevenire accessi dannosi o inappropriati ai sistemi di SCM Group.

MINIMIZZARE RISCHI DA VIRUS E CORRUZIONI DEI DATI DA TERZE PARTI

Le terze parti che accedono ai sistemi di SCM Group devono accettare di compiere ogni ragionevole sforzo per scansionare qualsiasi materiale destinato alla trasmissione elettronica in qualsiasi formato

elettronico (es., email, file transfer, flash drive, etc.) da virus e/o altri programmi informatici dannosi prima del suo trasferimento a SCM Group.

CONTROLLO ACCESSI EXTRANET O INTERNET

Le connessioni extranet o internet devono essere protette da un dispositivo firewall approvato che limiti l'accesso solo ai componenti necessari come server Web, sistemi di posta elettronica o altri fino all'indirizzo IP e al livello di porta. Inoltre, i gateway applicativi devono essere forniti ove tecnicamente fattibile per limitare ulteriormente l'accesso alle funzioni e alle transazioni necessarie.

COLLEGAMENTI DIRETTI CON RETI ESTERNE (TUNNELS)

Il team di sicurezza di SCM Group (*IT Infrastructure & Security team*) deve approvare la creazione di connessioni dirette tra i sistemi di SCM Group e i sistemi di organizzazioni esterne, tramite Internet o qualsiasi altra rete pubblica/privata prima della loro implementazione.

ACCESSO INTERNET IN USCITA

Tutti gli accessi Internet in uscita devono essere approvati dal team I*T Infrastructure & Security Team*.

ACCESSO REMOTO BASATO SU INTERNET

Tutti i metodi di accesso remoto in entrata basati su Internet alle reti interne di SCM Group e/o ai sistemi informatici multiutente devono essere approvati dal Team *IT Infrastructure & Security Team*. L'applicazione di uno specifico meccanismo di autenticazione deve essere basata su criteri stabiliti dal Team I*T Infrastructure & Security Team* per includere:

- La criticità della risorsa del sistema informativo di destinazione
- Tipologia di utente: Dipendente, Ex dipendenti, Contractor, Partner fornitore o Partner commerciale
- La classificazione SCM Group delle informazioni a cui accedere
- L'accesso remoto da parte di dipendenti non appartenenti a SCM Group seguirà l'accesso con privilegi minimi, assegnando l'accesso ai sistemi di SCM Group in base alle necessità e alla separazione dei compiti.

PROTOCOLLI

Tutti i dispositivi in rete devono utilizzare solo meccanismi di autenticazione crittografati, salvo diversa autorizzazione del team *IT Infrastructure & Security Team*. I servizi che utilizzano l'autenticazione non crittografata (come, ad esempio, Telnet) devono essere sostituiti dai loro equivalenti crittografati o implementati in modo sicuro come viaggiare attraverso un tunnel sicuro end-to-end o operare su una rete completamente privata.

Qualsiasi esigenza aziendale per l'utilizzo di protocolli che utilizzano un meccanismo di autenticazione non crittografato devono essere documentati e approvati dal team *IT Infrastructure & Security Team*.

POSTA ELETTRONICA

Tutta la posta Internet deve essere fornita tramite un server di posta approvato da SCM Group. Tutti i file devono essere sottoposti a scansione antivirus prima di essere introdotti nell'infrastruttura informatica e di comunicazione di SCM Group.

PRIVILEGI DI SICUREZZA PER L'UTILIZZO DI INTERNET

Per gestire il costo dei servizi Internet e la loro continua disponibilità a supporto delle attività commerciali, SCM Group si riserva il diritto di limitare o revocare i privilegi Internet dei dipendenti laddove i livelli di

utilizzo o le attività siano ritenuti inappropriati o incoerenti con le politiche, le linee guida o i principi fondamentali di SCM Group i valori. SCM Group si riserva il diritto di limitare o revocare i privilegi Internet a propria discrezione.

NAVIGAZIONE INTERNET

SCM Group blocca le connessioni a determinati siti Web non aziendali. I collegamenti involontari a siti contenenti ad esempio materiale sessualmente esplicito, razzista, violento o altro materiale offensivo devono essere immediatamente interrotti. La connettività ai siti web non implica di per sé che gli utenti dei sistemi di SCM Group siano autorizzati a visitare tali siti.

8.2 USER ACCESS MANAGEMENT

GENERALE

DIVIETI SUGLI ACCOUNT UTENTE

Gli Account Utente condivisi non devono essere creati o emessi senza l'approvazione dell'*IT Infrastructure & Security Team*. Gli Account Utente condivisi devono avere un proprietario designato del gruppo SCM e devono essere ricertificati annualmente. Gli Account Utente di processi, gli Account Utente utilizzati al solo scopo di elaborazione batch, processi automatizzati o altre funzioni non interattive, non devono essere creati o emessi senza l'approvazione dell'*IT Infrastructure & Security Team*. Gli Account Utente di processo devono avere proprietari del gruppo SCM designati validi e devono anch'essi essere ricertificati annualmente. Gli account predefiniti (utente e amministratore) forniti con il software devono essere rimossi, disabilitati o rinominati ove tecnicamente fattibile. Laddove non tecnicamente fattibile (ad es. root, sysdba), i controlli approvati dall' *IT Infrastructure & Security Team* devono essere attuati per mitigare il rischio, inclusa, ma non limitata a, la modifica delle password predefinite.

GRUPPI UTENTE

L'accesso alle risorse dovrebbe essere per definizione a livello di gruppo e dovrebbe essere legato alla funzione lavorativa, all'area aziendale e alla necessità di conoscere/privilegio minimo.

PROCESSO DI CONCESSIONE E REVOCA DELL'ACCESSO

RICHIESTE DI ACCESSO

A meno che non sia specificamente identificata come risorsa predefinita concessa come parte del rapporto di lavoro con la società, il responsabile dell'utente e il proprietario delle risorse richieste (ove tale proprietario esista) devono esaminare e approvare tutte le richieste di accesso. Al momento dell'assegnazione di un nuovo account, il nuovo utente deve essere tenuto a riconoscere di aver compreso le proprie responsabilità in quanto utente di un patrimonio informativo di SCM Group.

NOTIFICA IN CASO DI TRASFERIMENTO O RISOLUZIONE DELL'UTENTE

La Direzione Risorse Umane o la Direzione Aziendale devono comunicare immediatamente alla Direzione IT le dimissioni, la cessazione o il trasferimento del personale, o la cessazione del loro rapporto d'affari con SCM Group. L'attuale supervisore del dipendente trasferito o licenziato è responsabile del coordinamento diretto della rimozione dei diritti di accesso dell'utente. Ciò vale anche per tutti i consulenti, appaltatori e personale temporaneo. In caso di notifica di trasferimento o cessazione del personale da parte delle Risorse Umane o della direzione aziendale, l'accesso deve essere rimosso entro un giorno lavorativo.

NOTIFICA DI ANOMALIE PRIVILEGI DI ACCESSO

Il dipendente è invitato a segnalare tempestivamente eventuali difformità tra privilegi d'accesso e mansioni svolte che si verifichino nel corso della naturale evoluzione del rapporto di lavoro (a titolo esemplificativo, cambiamento di mansioni legato ad esigenze operative oppure modifica del reparto, dipartimento, o ambito aziendale).

Ogni anomalia di funzionamento deve essere immediatamente segnalata all'Amministratore di Sistema o ad altro responsabile IT, che effettuerà le opportune verifiche e valutazioni.

REVISIONE DELL'ACCESSO ALL'ACCOUNT PRIVILEGIATO

È necessario condurre revisioni **annuali** degli accessi degli account utente privilegiati per garantire che quelli non autorizzati vengano rimossi.

REVISIONE ADS (AMMINISTRATORI DI SISTEMA).

Le revisioni **annuali** dell'elenco degli ADS, interni ed esterni all'organizzazione, devono essere condotte dal Team *IT Infrastructure & Security* per verificarne la conformità alle misure organizzative, tecniche e di sicurezza rispetto al trattamento dei dati personali richieste dalla normativa europea vigente.

AUTENTICAZIONE STANDARDIZZATA (SSO)

Tutti i sistemi devono integrarsi e ove possibile fare affidamento sul sistema standard di autenticazione (SSO) aziendale approvato dal team *IT Infrastructure & Security*.

CONTROLLI DI IDENTIFICAZIONE

RILASCIO ID UTENTE

Gli ID utente devono essere univoci e assegnati a un individuo indipendentemente dalla piattaforma di elaborazione. Per tutti gli ID utente emessi, SCM Group deve conservare i record con il nome completo, la relazione con SCM Group e le informazioni di contatto.

COMPOSIZIONE ID UTENTE SCM GROUP

Gli ID utente devono essere costituiti dal primo carattere del nome e del cognome e, se richiesto per unicità, utilizzare il primo carattere del secondo nome (se disponibile) o il secondo/terzo carattere del nome. Di seguito un esempio; i campi tra parentesi sono facoltativi ai fini dell'univocità:

<iniziale nome>(<secondo carattere>)(<terzo carattere>)<cognome>

DESIGNAZIONE PERSONALE NON SCM

Il personale non appartenente a SCM Group, come consulenti, contractors e dipendenti temporanei, deve essere facilmente identificabili come utente non appartenente a SCM Group a chiunque all'interno dell'azienda. Qualsiasi e-mail inviata deve essere chiaramente contrassegnata come non appartenente a SCM Group o alla rispettiva società.

CREDENZIALI INCORPORATE

Gli ID utente e/o le relative password non devono essere incorporati in file batch o script che automatizzano le sequenze di autenticazione.

ACCOUNT INATTIVI E SCADENZA ACCOUNT

Ove tecnicamente fattibile, gli account utente di SCM Group rimasti inattivi per più di 90 giorni e gli account utente non SCM Group che sono rimasti inattivi per più di 60 giorni devono essere disabilitati. Un account deve rimanere disabilitato fino a quando l'utente specificato non richiede all'helpdesk che l'account venga

riabilitato e fornisce una prova di identità, inclusa la prova che il suo rapporto commerciale con SCM Group non è cambiato. Per gli utenti non SCM Group, deve essere stabilita una data di scadenza dell'account impostata dal sistema che coincida con la conclusione del progetto o **6 mesi**, se inferiore.

ACCOUNT PRIVILEGIATI

Gli utenti con accesso privilegiato (root, amministratore, ecc.) devono utilizzare un nome account diverso da quello di un utente normale. Questi ID devono essere riconvalidati **ogni 1 anno.**

SOSPENSIONE DELL'ACCOUNT DI SISTEMA PER TENTATIVI DI ACCESSO NON RIUSCITI

Ove possibile. Dopo 10 tentativi di accesso falliti consecutivi, un account utente deve essere bloccato per 15 minuti o fino a quando non viene ripristinato manualmente dall'amministratore della sicurezza delle informazioni.

USO ERRATO DI IDENTITÀ

È vietato travisare, oscurare o sopprimere l'identità di un utente (anonimato) su qualsiasi sistema di comunicazione.

8.3 GESTIONE CREDENZIALI D'ACCESSO

L'accesso ai dati è consentito solo dopo il superamento di una procedura di autenticazione. È opportuno che la password scelta dall'incaricato sia tale da garantire la massima protezione secondo quanto stabilito dalla procedura "*2SCM - Password Policy*" definita ed approvata da SCM Group.

MEMORIZZAZIONE PASSWORD

Le credenziali di accesso personali devono essere mantenute segrete, pertanto è assolutamente vietato salvarle in chiaro (sia su file che su supporto cartaceo) o comunicarle ad un altro dipendente o a terzi in genere.

COMPOSIZIONE/COMPLESSITÀ DELLA PASSWORD

Le password devono essere composte da un **minimo di 16 caratteri.**

- Le password devono essere costruite utilizzando almeno 3 dei seguenti tipi di carattere:
  - Caratteri minuscoli (incluse le lettere dell'alfabeto inglese);
  - Caratteri maiuscoli (incluse le lettere dell'alfabeto inglese);
  - Caratteri numerici;
  - Punteggiatura e simboli speciali disponibili nelle tastiere di utilizzo comune;
- Nei casi in cui non risulti possibile l'utilizzo dei simboli speciali, le password devono contenere caratteri numerici ed alfabetici ripartibili in numero compreso tra un minimo di 3 ed un massimo di 5, ferma restando la lunghezza minima complessiva fissata in 16 caratteri;
- Le password non devono contenere più di tre caratteri uguali consecutivi;
- Le password non devono contenere caratteri di spaziatura, in alcuna posizione;
- Non sono ammesse password:
  - Uguali al corrispettivo identificativo utente;
  - Contenenti il nome o il cognome della persona proprietaria;
  - Contenenti la matricola aziendale della persona proprietaria.

CAPACITÀ DELL'UTENTE DI MODIFICARE LE PASSWORD

Agli utenti deve essere fornita la possibilità di modificare la propria password dopo l'accesso.

UTILIZZO ONE-TIME USE DELLA PASSWORD INIZIALE

Se a un utente viene fornita da SCM Group una password iniziale, questa **deve essere cambiata la prima volta che un utente accede a un servizio.** Ove possibile, il sistema deve applicare la modifica iniziale fino alla scadenza anticipata. Le password temporanee devono essere trasmesse agli utenti in modo sicuro e affidabile.

ETA' MINIMA DELLA PASSWORD

Le password devono avere **un'età minima di 1 giorno** ove tecnicamente fattibile.

SCADENZA PASSWORD

Le password per gli utenti **devono scadere dopo 90 giorni.** I sistemi devono avvisare l'utente quotidianamente, a partire da almeno 15 giorni prima, quando la sua password scadrà. Un account con una password scaduta deve essere forzato a cambiare la password al prossimo accesso.

RESET PASSWORD

Saranno accettate solo le richieste di ripristino dal singolo titolare dell'account o da un delegato approvato dal team *IT Infrastructure & Security Team.*

PASSWORD HISTORY

Agli utenti non deve essere consentito selezionare una password che corrisponda a una delle **5 password precedenti** dell'utente.

ECCEZIONI

SCM Group riconosce che, a volte, alcuni controlli di autorizzazione, identificazione o password potrebbero non essere applicabili a tutti gli utenti. L'approvazione del team *IT Infrastructure & Security* è richiesta e deve essere documentata per tutti questi casi.

8.4 CONTROLLO DEGLI ACCESSI ALLA RETE

CONNESSIONE DEI SERVER

I server non devono essere configurati per l'accesso alla rete senza l'approvazione del team *IT Infrastructure & Security*.

ACCESSO SISTEMI ALLA RETE

Tutti gli host che archiviano o elaborano i dati SCM Group devono essere isolati dietro un firewall dalle reti pubbliche esterne (ad es. Internet). Gli amministratori di sistema devono limitare l'accesso da e verso le porte e gli indirizzi IP pertinenti.

REVISIONE DEGLI ACCESSI AI SERVER DALL'ESTERNO

I set di regole del firewall e del router devono essere rivisti su base annuale per rilevare modifiche non autorizzate.

FILTRAGGIO DEL TRAFFICO DI RETE

Il traffico di rete deve essere filtrato in base a quanto determinato dal team *IT Infrastructure & Security*. Il traffico da vietare deve includere tutto il traffico non giustificato dall'attività e tutto ciò che è proibito dalle policy di SCM Group.

INVENTARIO DELLE CONNESSIONI ESTERNE ALLA RETE

Un inventario di tutte le connessioni esterne alla rete deve essere mantenuto dal reparto IT di SCM Group e deve essere rivisto regolarmente.

CONNETTIVITÀ VERSO E TRA LE RETI

IT Infrastructure & Security Team deve autorizzare tutte le nuove connessioni a reti wireless e cablate che potrebbero consentire agli utenti di accedere ai sistemi e alle informazioni di SCM Group.

Se la nuova connessione è un'aggiunta a una connessione interna o esterna precedentemente certificata e la connessione viene effettuata utilizzando la stessa configurazione, non è richiesta alcuna approvazione preventiva. Tutte le connessioni tra reti interne e Internet (o qualsiasi altra rete informatica accessibile al pubblico) devono incorporare un dispositivo firewall approvato e i relativi controlli di accesso.

AMMINISTRAZIONE SISTEMI CON ACCESSO DA REMOTO

Tutta l'amministrazione dei sistemi non effettuata da una console deve essere condotta utilizzando metodi sicuri che sono stati approvati dal team *IT Infrastructure & Security* e dovrebbero ove possibile utilizzare l'autenticazione a due fattori (MFA) quando possibile.

GESTIONE RETI WIRELESS

Tutte le reti wireless devono essere pianificate, implementate e gestite in modo organizzato e centralizzato per garantire funzionalità, larghezza di banda massima, gestione delle interferenze e sicurezza. Pertanto, il team *IT Infrastructure & Security* è l'unico responsabile dell'implementazione dell'accesso wireless destinato all'uso sulla rete aziendale di SCM Group. Anche l'accesso wireless a reti non aziendali (ad es. accesso Guest) deve essere esaminato e approvato dal team *IT Infrastructure & Security.*

Le trasmissioni wireless devono utilizzare una crittografia avanzata per l'autenticazione e la trasmissione dei dati di SCM Group.

Tutte le implementazioni wireless sulla rete di SCM Group devono essere approvate dal team *IT Infrastructure & Security.*

MODEM WIFI POLICIES

I modem WiFi non devono essere acquistati o installati nei computer senza l'approvazione del team *IT Infrastructure & Security*

Tutte le connessioni con modem WiFi devono essere configurate solo per l'accesso in uscita, a meno che non si ottenga un'autorizzazione scritta dal team *IT Infrastructure & Security*.

L'approvazione per l'installazione del software di comunicazione di controllo remoto (software che consente a un utente remoto di connettersi a un PC collegato alla rete e di impartire comandi da esso come se fosse collegato alla rete stessa) deve essere approvata in anticipo dal team *IT Infrastructure & Security*.

8.5 CONTROLLO ACCESSI SISTEMA OPERATIVO

CONTROLLO DI ACCESSO

I permessi di file e directory devono essere rivisti e ridotti al minimo necessario, secondo il principio "Need-to-Know", al fine di fornire la funzionalità del servizio pertinente.

CONFIGURATIONE STANDARD SISTEMA OPERATIVO

Tutti i sistemi devono essere configurati secondo gli standard di configurazione approvati dal team *IT Infrastructure & Security*

SINGOLO UTILIZZO

Tutti i sistemi dovrebbero essere implementati per svolgere una funzione primaria.

MESSAGGIO DI AVVISO DI SISTEMA E BANNER DI ACCESSO

Dove tecnicamente fattibile, deve essere visualizzato un messaggio a tutte le connessioni di rete che avverte i potenziali utenti che l'uso non autorizzato è proibito. I banner di accesso o le schermate di saluto non devono rivelare alcuna informazione di sistema.

8.6 CONTROLLO DELL'ACCESSO ALLE APPLICAZIONI AZIENDALI

Al dipendente sono assegnati, a seconda del ruolo in azienda, accessi e credenziali ad applicazioni aziendali che potrebbero contenere informazioni riguardo dati personali dei dipendenti oppure a documentazione aziendale confidenziale.

Qualora il dipendente nel corso della sua vita professionale, si dovesse accorgere di avere accesso ad informazioni che per il ruolo attualmente rivestito non siano più di sua competenza o che nel tempo non lo sono più, deve immediatamente riferire al reparto IT aziendale tale situazione, affinché vi si ponga rimedio nel più breve tempo possibile.

9. SICUREZZA DEI SISTEMI INFORMATICI PER ACQUISIZIONE, SVILUPPO E MANUTENZIONE DELLE INFORMAZIONI AZIENDALI

9.1 REQUISITI DI SICUREZZA DEI SISTEMI INFORMATIVI

SECURITY BY DESIGN

I sistemi, gli standard e le piattaforme di SCM Group devono essere implementati considerando la sicurezza fin dalla progettazione. I Business Analyst ed i Business Process Owner hanno la responsabilità congiunta di garantire che le linee guida sulla sicurezza siano parte integrante del processo di progettazione, test, installazione e distribuzione dei sistemi. I problemi di sicurezza e l'impatto devono essere affrontati e documentati.

DESIGN

CONTROLLI DI SICUREZZA DELLE INFORMAZIONI IDENTIFICAZIONE/DOCUMENTAZIONE

Tutte le caratteristiche di sicurezza devono essere identificate e documentate prima dell'installazione e dell'uso. La documentazione del prodotto finale deve includere una spiegazione delle funzionalità di sicurezza del software in modo che possano essere utilizzate in modo efficace.

9.2 CORRETTA ELABORAZIONE NELLE APPLICAZIONI

SVILUPPO

Controlli appropriati devono essere progettati nelle applicazioni, comprese le applicazioni sviluppate dall'utente per garantire un'elaborazione corretta. Questi controlli dovrebbero includere la convalida dei dati di input, l'elaborazione interna, i dati di output e la registrazione.

TESTING DELLE CARATTERISTICHE DI SICUREZZA

Il test delle funzionalità di sicurezza deve essere eseguito come parte del test del sistema. Le funzionalità di sicurezza documentate nei requisiti di sicurezza e nella progettazione della sicurezza i devono essere completamente testate utilizzando scenari sviluppati durante la fase di progettazione. I risultati dei test devono essere completamente documentati e conservati per tutta la vita del sistema.

9.3 SICUREZZA DEL SOFWTARE

SOFTWARE SECURITY

I dipendenti di SCM Group e gli utenti dei sistemi e delle risorse di SCM Group devono utilizzare solo software autorizzato dal Dipartimento IT. Il software protetto da copyright deve essere utilizzato in conformità con i requisiti specificati nel contratto di licenza o in qualsiasi accordo firmato con SCM Group. Gli utenti non devono copiare o modificare il software acquistato se non espressamente previsto nella licenza del software. I prodotti concessi in licenza per essere eseguiti su un computer specifico o presso un sito particolare non devono essere copiati su un altro computer o utilizzati presso un altro sito senza l'autorizzazione scritta del fornitore. Il software copiato o scaricato illegalmente da una fonte non autorizzata non può essere caricato su apparecchiature di proprietà di SCM Group. Se sono necessari programmi di dominio pubblico o distribuiti in massa (ad esempio, driver di stampa) per una valida esigenza aziendale, è necessario ottenerli da una fonte attendibile come un sito di un fornitore.

SOFTWARE PROPRIETARIO

Prima di distribuire il software di proprietà di SCM Group a terzi, è necessario ottenere l'autorizzazione dall'ufficio legale e dal vendor del software stesso.

9.4 SICUREZZA NEI PROCESSI DI SVILUPPO E DI SUPPORTO

SEPARAZIONE AMBIENTI DI TEST E QA DALL'AMBIENTE DI PRODUZIONE

Le funzioni di test e QA devono essere tenute separate fisicamente o logicamente dagli ambienti di produzione.

10. GESTIONE DELLA RISPOSTA AGLI INCIDENTI DI SICUREZZA

RISPOSTA ALL'INCIDENTE

Fare riferimento al documento "*SCM Group - Incident Response Plan*" per tutti dettagli e le procedure.

ISOLAMENTO DEGLI INCIDENTI

Gli amministratori di sistema devono intraprendere le azioni necessarie per limitare gli effetti di un incidente di sicurezza attraverso l'isolamento immediato del problema.

11. BUSINESS CONTINUITY MANAGEMENT

Fare riferimento al documento "*Disaster Recovery Strategy SCM Group*" per maggiori informazioni.

12. TRAINING

SCM Group organizza periodicamente corsi di formazione sulla sicurezza IT per tutti i dipendenti (e comunque all'assunzione dei nuovi dipendenti) per comprendere meglio come utilizzare gli strumenti informatici, le misure di sicurezza adottate e da adottare, le procedure o misure di sicurezza da implementare.

Il dipartimento IT sarà responsabile di tutti i contenuti dei corsi e, a seconda dell'argomento, saranno organizzati attraverso la piattaforma di formazione aziendale o in aula.

La formazione deve prevedere una verifica dell'effettiva comprensione dei contenuti presentati (deve essere inclusa la fase di valutazione); la certificazione di partecipazione, con gli esiti della verifica, deve essere documentata e conservata per eventuali future verifiche.