Sicurezza dei sistemi informativi

	Funzione	Responsabile	Data
Elaborato da:	IT Department	M.Corsi / A.Folco	03/06/2024
Verificato da:	Chief Information Officer	E. Turra	03/07/2024
Approvato da:	CFO & Head of Corporate Services	R. Ruella	01/08/2024

AGGIORNAMENTI

Data	Versione	Descrizioni	Cap./Sez. modificati
01/10/2012	Rev.00	Prima emissione Protocollo (A. Zambon – G. Bonin)	-
28/10/2014	Rev.01	Sistema delle deleghe e delle procure – tabella riepilogativa	Cap. 5
22/10/2018	Rev.02	Revisione generale del documento a seguito dell'aggiornamento del Modello Organizzativo	-
01/08/2024	Rev. 03	Revisione generale del documento	-

INDICE

1. SCOPO

Il presente documento ha lo scopo di definire i ruoli, le responsabilità, le modalità operative e i principi comportamentali cui tutto il personale della Società AFV Acciaierie Beltrame S.p.A. (di seguito "AFV Beltrame" o la "Società") deve attenersi nella gestione della sicurezza dei sistemi informativi della Società, con la finalità di descrivere le attività necessarie a prevenire accessi non autorizzati alle informazioni ed ai sistemi informatici aziendali ovvero a garantire che questi siano protetti non solo fisicamente, ma che siano implementate adeguate misure di sicurezza logica, ovvero modalità e tecniche di controllo e di tracciamento degli accessi utenti.
La procedura, redatta in conformità ai requisiti indicati dal D.Lgs. n. 231/2001, costituisce parte integrante del Modello di Gestione, Organizzazione e Controllo previsto dal Decreto medesimo.

2. AMBITO DI APPLICAZIONE

Il presente documento si applica a tutto il personale della Società che, nell'espletamento delle attività di propria competenza e a vario titolo, è coinvolto nell'utilizzo e nella gestione delle risorse informatiche aziendali.
Per controllo logico degli accessi devono intendersi le attività volte a garantire che tutti gli accessi ai sistemi informativi avvengano esclusivamente secondo modalità prestabilite. Tali attività devono fornire un modo tecnico per controllare l'accesso di un utente alle risorse di sistema e alle informazioni, al fine di garantire il controllo delle informazioni che gli utenti possono utilizzare, dei programmi che possono eseguire e delle modifiche che possono apportare.

3. PRINCIPI GENERALI DI COMPORTAMENTO E CONTROLLO

Il personale della Società a qualsiasi titolo coinvolto nel processo in oggetto è tenuto ad osservare le modalità esposte nella presente procedura, le previsioni di legge esistenti in materia e le previsioni contenute nel Codice Etico della Società e nel Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 adottato dalla Società nonché le regole elaborate dalla Direzione IT e pubblicate nella Intranet aziendale. In particolare, è fatto divieto di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informativi o telematici altrui o ostacolarne gravemente il funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- costringere a fare o omettere qualcosa, mediante violenza o minaccia, al fine di procurare un ingiusto profitto con altrui danno mediante il compimento, o la minaccia di compiere, talune delle condotte vietate sopra descritte;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno;
- duplicare programmi per elaboratore o importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE) o in assenza del pagamento dei relativi diritti e/o licenze di terzi.

In linea generale, i principi che regolano la sicurezza delle informazioni in azienda sono i seguenti:

1) l'accesso alle informazioni che risiedono sui server e sulle banche dati aziendali, ivi inclusi i client, è limitato da idonei strumenti di autenticazione;
2) gli amministratori di sistema e gli addetti alla manutenzione sono muniti di univoche credenziali di autenticazione;
3) l'accesso alle applicazioni, da parte del personale IT, è garantito attraverso idonei strumenti di autorizzazione. I profili di autorizzazione, strettamente limitati alle mansioni degli amministratori e degli utenti, sono rivisti dal responsabile di funzione a fronte di cambio mansione
4) i server, i laptop, gli smartphone e gli altri dispositivi aziendali che prevedono *patching* sono aggiornati, qualora necessario, sulla base delle *patch* rilasciate dai produttori dei sistemi operativi;

5) la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (come *firewall*, *proxy o altri strumenti adeguati*) e da adeguati strumenti di monitoraggio contro il rischio di accesso abusivo, di cui all'art. 615 ter del Codice penale;
6) i dispositivi telematici di instradamento sono collocati in aree dedicate e protetti al fine di renderli accessibili al solo personale autorizzato;
7) tutti i server ed i computer aziendali sono protetti da programmi antivirus e da sistemi evoluti di protezione degli *end point* con software XDR (*Extended Detection and Response* o altri strumenti adeguati) contro il rischio di intrusione, aggiornati in modo automatico;
8) il personale deve astenersi dal diffondere le informazioni ricevute dalla Società per l'uso dei mezzi informatici aziendali e l'accesso a dati, sistemi e applicazioni aziendali;
9) il personale deve attuare i comportamenti richiesti e incoraggiati dalla Società nell'ambito delle attività di formazione e necessari per proteggere il sistema informativo;
10) il personale deve accedere al sistema informativo aziendale unicamente attraverso i codici di identificazione prescelti, provvedendo alla modifica periodica tutte le volte in cui il sistema lo richieda e a intervalli regolari, come disciplinato dalle procedure interne e/o dalle normative vigenti;
11) il personale è munito di univoche credenziali di autenticazione. I codici identificativi devono essere conservati astenendosi dal comunicarli a terzi che potrebbero accedere abusivamente a dati aziendali riservati;
12) il personale deve astenersi da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni e dei dati aziendali;
13) il personale deve astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui;
14) il personale non può installare applicazioni o software senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica o senza preventivi accordi, verifiche ed eventuali deroghe con la funzione stessa

Qualora il rapporto della Società nell'ambito delle attività connesse alla sicurezza dei sistemi informativi sia gestito anche attraverso professionisti esterni ovvero studi associati o società di consulenza, etc., a questi ultimi viene preventivamente richiesta la sottoscrizione di una dichiarazione di conoscenza della normativa di cui al D.Lgs. 231/2001, del Codice Etico di Gruppo e di impegno al loro rispetto.

3.1 Violazioni del Protocollo

Ogni violazione delle regole di comportamento del presente protocollo costituisce violazione del Modello di Organizzazione, Gestione e Controllo ed è sanzionata in proporzione alla gravità dell'infrazione commessa e all'esposizione al rischio che ne dovesse derivare anche per gli altri lavoratori, in ogni caso nel rispetto delle procedure disciplinari previste nel CCNL applicabile e nel Sistema Sanzionatorio previsto nel Modello.

4. MODALITÀ OPERATIVE

4.1 Password utente

4.1.1 Regole generali per la gestione delle password utente

Le password sono utilizzate per validare l'identità di un utente prima di concedergli l'accesso a sistemi e/o informazioni. La concessione di password all'interno della Società è controllata tramite un processo di gestione formale. Tale processo prevede quanto segue:

- l'associazione di una sola credenziale ad utente per l'autenticazione iniziale al sistema informativo;
- la diffusione di istruzioni relative alla gestione e conservazione delle credenziali utente;
- la sicurezza delle modalità di comunicazione delle password agli utenti con conferma, anche verbale, da parte degli stessi, in merito alla ricezione delle password;
- l'utilizzo di specifiche soluzioni tecnologiche e meccanismi di autenticazione in grado di verificare la validità del codice identificativo utente e della password dichiarati, proteggendo la riservatezza della password, soprattutto nel caso in cui questa debba essere trasmessa tramite la rete;
- un sistema di autenticazione adeguato alla criticità delle informazioni da proteggere.

4.1.2 Sistema di gestione delle password

Il sistema di gestione delle password utente implementato da AFV Beltrame contempla i seguenti requisiti:

- consentire l'utilizzo e riconoscere le sole password "di qualità" (ove il sistema lo consenta), costituite ad esempio da codici alfanumerici sia maiuscoli sia minuscoli nonché caratteri speciali;
- definire di una lunghezza minima;
- consentire agli utenti di modificare la propria password;
- forzare gli utenti a cambiare la password al primo login, nel caso di password temporanee assegnate per il primo accesso a un sistema;
- suggerire il cambiamento con periodicità prestabilita;
- non permettere l'utilizzo di password già utilizzate;
- visualizzare solo asterischi o simboli analoghi al posto dei caratteri, quando si digita la password;
- disporre di un elenco criptato delle password di specifici sottosistemi IT.

4.2 Controllo profili autorizzativi

Al fine di mantenere un controllo efficiente ed efficace sugli accessi alle informazioni e ai sistemi è necessario condurre periodiche *review* formali tali che:

- i diritti di accesso utenti siano controllati ad ogni cambiamento di ruolo, su indicazione della Funzione Human Resources;

- i diritti di accesso vengano disattivati se non utilizzati da più di 6 mesi, salvo per le utenze preventivamente autorizzate o per soli scopi di gestione tecnica o per esigenze specifiche.

4.3 Controllo d'accesso a livello di sistema operativo

4.3.1 Login alle postazioni computer di lavoro

L'accesso ai sistemi informativi aziendali è consentito solo a seguito di un processo di login sicuro. La procedura di login è stata appositamente progettata per minimizzare le possibilità di accessi non autorizzati. I messaggi visualizzati riportano il minimo di informazioni possibili sul sistema in modo da non fornire ad un utente non autorizzato informazioni che potrebbero in qualche modo aiutarlo ad accedere.
Nel processo di login sono stati considerati i seguenti aspetti:

- non mostrare identificativi del sistema o delle applicazioni finché il processo di login non è stato portato a termine con successo;
- autenticare l'utente solo una volta che tutte le informazioni sono state inserite correttamente e, in caso di errore, non specificare nell'inserimento di quale dato è stato commesso l'errore, ma riportare soltanto che il tentativo di login è fallito.

4.4 Controllo d'accesso a livello applicativo

4.4.1 Restrizioni nell'accesso alle informazioni ai soli utenti abilitati

Sono previsti i seguenti controlli al fine di restringere l'accesso alle informazioni ai soli utenti abilitati:

- limitare l'accesso ai sistemi applicativi da parte degli utenti appartenenti a funzioni aziendali che non sono autorizzate all'utilizzo degli stessi;
- controllare i diritti di accesso degli utenti, se in semplice lettura e/o scrittura (sempre e comunque direttamente dai vari server).
- verificare, su indicazione della Funzione Human Resources, che i diritti di accesso a livello applicativo ai dati o alle funzioni siano coerenti con i ruoli/ mansioni dell'utente.

4.5 Autenticazione degli utenti per gli accessi remoti

4.5.1 Generalità

Le connessioni da remoto di utenti esterni costituiscono una potenziale minaccia di accessi non autorizzati alla rete aziendale e devono pertanto essere controllate predisponendo sistemi di autenticazione specifici (i.e. MFA, VPN e altre tecnologie di sicurezza disponibili).

4.5.2 Controlli

Il sistema di controllo delle connessioni è interamente gestito dalla Società . L'accesso alle reti della Società è garantito attraverso l'utilizzo di apposito gateway di accesso. Tutti gli accessi sono tracciati dalla Direzione IT che, in caso di problemi, controlla i relativi *log* di connessione.

4.6 Sistemi di monitoraggio (logging)

L'accesso ai sistemi è oggetto di monitoraggio al fine di individuare attività non autorizzate dalle regole di accesso ai sistemi e registrare eventi significativi utili per l'acquisizione di prove in caso di incidenti di sicurezza.

4.6.1 Logging degli eventi

I sistemi producono *event-log* dei controlli d'accesso riportanti eventuali anomalie e altri eventi rilevanti ai fini della sicurezza. Tali *log* sono conservati per un determinato periodo di tempo come materiale di supporto per controlli successivi.
Periodicamente la Direzione IT controlla il sistema di generazione dei log:

- per prevenire eventuali malfunzionamenti;
- per rilevare atti dolosi;
- per evitare che vengano modificati i messaggi di *alert* prodotti;
- per evitare che siano cancellati o modificati determinati file di *log*.

La gestione dei *log* ed il loro monitoraggio è di competenza della Direzione IT, che si avvale inoltre del supporto di società specializzate di consulenza esterna che forniscono servizio di monitoraggio continuo (24h, 7/7), e il tracciamento degli accessi alle reti societarie avviene su server la cui amministrazione è consentita al solo personale autorizzato da parte di detta Direzione.

4.6.2 Monitoraggio dell'utilizzo dei sistemi

Tali attività sono svolte dalla Direzione IT, con il supporto di consulenti esterni competenti in materia, e i relativi esiti (anomalie, criticità) vengono comunicati sistematicamente all'Organismo di Vigilanza.

4.7 Gestione hardware e software

La configurazione della dotazione software installata su tutti i computer della Società è sviluppata, e interamente gestita, dalla Direzione IT (ad esclusione di alcune aree tecniche al di fuori della responsabilità di detta Direzione). L'elenco dei *software* di tale configurazione è disponibile presso la Direzione IT.
I software sono installati sui computer, sui devices e sulle reti aziendali esclusivamente da personale autorizzato a svolgere questo genere di operazioni. L'installazione di software non approvati e/o privi di regolare licenza non è consentita in nessun caso, nel rispetto delle procedure interne (*Regolamento per l'utilizzo dei beni e dei servizi informativi*) e/o delle normative vigenti.

Inoltre, la Direzione IT verifica periodicamente tramite specifico *software* l'eventuale installazione, da parte dei dipendenti, di *app* o *software* su computer o *devices* aziendali al fine di intercettare la presenza di applicativi non autorizzati o rispetto ai quali non sono stati gestiti i relativi diritti d'uso (i.e. licenze d'uso).
In ultimo, la Direzione IT aggiorna e conserva, con l'ausilio di applicativi informatici *ad hoc*, il database delle apparecchiature *hardware IT* presenti nelle sedi societarie.

4.8 Gestione degli Account

4.8.1 Creazione Account

La creazione degli Account utente avviene secondo quanto disposto dalle normative aziendali. La Direzione IT riceve i dati necessari dalla Funzione Human Resources (nome e cognome, data di assunzione, posizione ricoperta, etc…) per la creazione di un nuovo account per ciascun nuovo assunto.
Sulla base di tali informazioni la Direzione IT provvede alla creazione della nuova *username* e la inserisce nel rispettivo gruppo/*distribution list* di appartenenza.
La *password* creata viene comunicata all'utente; è responsabilità dell'utente modificare la *password* in occasione del primo accesso e crearne una nuova.
L'approvazione della richiesta di ulteriori *software* rispetto al set standard previsto e la relativa installazione è responsabilità della Direzione IT.

4.8.2 Cessazione Account

In caso di cessazione del rapporto di lavoro, la Funzione Human Resources comunica alla Direzione IT i dati del dipendente in uscita affinché vengano realizzate le azioni necessarie al fine della cessazione dell'Account e della relativa casella di posta elettronica.

4.8.3 Accesso ai dati aziendali

L'accesso ai dati aziendali è gestito dai seguenti sistemi di sicurezza:

- account e password riservata;
- implementazioni di privilegi e/o profili autorizzativi.

Gli applicativi di base disponibili per i computer aziendali sono rappresentati da:

- programma di posta elettronica;
- software antivirus, firewall e XDR (o altri applicativi adeguati);
- applicativi MS Office;
- software gestionali (es. SAP, Pipeline);
- browser per la navigazione Internet, solo per gli utenti autorizzati dalle relative Direzioni;

- browser per la consultazione della Intranet, per cui tutti gli utenti risultano abilitati. Alcune Direzioni sono abilitate anche in scrittura limitatamente alle pagine di propria competenza, previa approvazione della Direzione IT;
- utilizzo di cartelle di rete, rappresentanti aree di rete protette relative al proprio ruolo/funzione;
- Sistema di archiviazione Documentale.

In ogni caso i profili di autorizzazione, per ciascun dipendente o per classi omogenee di dipendenti, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati e funzioni necessari per effettuare le operazioni di trattamento.

4.9 Back-up, Disaster Recovery e Cyber Security

4.9.1 Procedura di back-up

La Direzione IT è responsabile del processo di *back-up* aziendale.

4.9.2 Piano di Disaster Recovery

L'azienda dispone al suo interno di due unità, *data center* primario e *back-up room,* poste in palazzine diverse su diversi livelli/piani. Per limitare al massimo la possibilità di perdita dei dati e assicurare la continuità di servizio, nelle due sale sono presenti *server* e *storage* in ridondanza, configurati specularmente.
Sia i *server* del *data center* primario che i *server* della *back-up room* sono sempre attivi e bilanciano i carichi di lavoro richiesti dagli utenti, fornendo loro sufficienti risorse per assicurare adeguate *performance*. I dati vengono registrati contemporaneamente sia negli *storage* presenti nel *data center* primario che in quelli presenti nella *back-up room*.

In caso di compromissione dell'intera infrastruttura del *data center* primario, la *back-up room* è in grado di assicurare sia la consistenza dei dati che la continuità del servizio delle funzioni core, in quanto, sia i *server* che gli *storage* presenti possono vivere di vita propria.

I *server* e gli *storage*, sia del *data center* primario che della *back-up room*, sono oggetto di un contratto di assistenza che garantisce un tempo di risposta adeguato da parte dei fornitori. I fornitori monitorano i sistemi ed anticipano via e-mail alla Direzione IT eventuali guasti, aprendo il *ticket* per l'intervento tecnico.

Nel caso in cui quanto sopra indicato non sia sufficiente a far ripartire i sistemi della sala macchine principale (situazione di compromissione dell'intero sistema della sala principale), la sala secondaria è in grado di sopperire per i servizi CORE alle funzionalità richieste dagli utenti in quanto le macchine in essa collocate

prendono automaticamente in carico l'intero parco utenti che in quel momento sta utilizzando il sistema informativo, anche se con un degrado delle performance.

A fronte della continua evoluzione delle minacce e degli attacchi informatici, l'azienda adegua in maniera proattiva, e allineata ai *trend* di mercato, strumenti atti a prevenire gli attacchi e a garantire la resilienza dei sistemi informativi comprese eventuali soluzioni in *cloud* gestite nel rispetto degli accordi contrattuali definiti con i fornitori esterni che erogano tali servizi.

4.10 Rinvio

Si rinvia all'applicazione degli specifici protocolli di riferimento qualora dalla realizzazione delle attività normate nel presente protocollo derivino ulteriori attività già oggetto di regolamentazione da parte di altri protocolli (es. consulenze e prestazioni professionali, acquisto di beni e servizi, etc.).

5. SISTEMA DELLE DELEGHE E DELLE PROCURE

Ai fini dell'individuazione dei Responsabili e dell'identificazione dei poteri loro attribuiti, viene formalizzato un sistema di attribuzione di deleghe e procure che distribuisce le responsabilità e i compiti con riguardo al processo in esame.
Detto sistema è concepito in modo tale da facilitare, da un lato, un presidio capillare di tutte le aree e, dall'altro, un meccanismo di controllo gerarchico operativo.
Infatti è necessaria l'esistenza di livelli autorizzativi a garanzia di un adeguato controllo del processo decisionale, supportato da un sistema di deleghe e procure riguardante sia i poteri autorizzativi interni, dai quali dipendono i processi decisionali dell'azienda in merito alle operazioni da porre in essere, sia i poteri di rappresentanza per la firma di atti o documenti destinati all'esterno e idonei a vincolare la Società nei confronti dei terzi (cosiddette "procure" speciali o generali).
I responsabili così individuati devono esercitare, per l'area di loro competenza, tutti i poteri attribuiti ed adempiere a tutti gli obblighi previsti dalle leggi e regolamenti nella materia in argomento.
Nel Protocollo n. 0 "Sistema delle deleghe e delle procure" sono elencate le deleghe e le procure attualmente esistenti relative alla sicurezza dei sistemi informativi.
L'OdV sarà sistematicamente tenuto aggiornato dalla Direzione Corporate & Legal sui cambiamenti al sistema delle deleghe e procure in materia di consulenze e incarichi professionali tramite apposita modulistica (Report D 0-20 - Report di segnalazione all'OdV – "Elenco deleghe/procure attribuite").

6. FLUSSI INFORMATIVI ALL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza, istituito ai sensi del D.Lgs. 231/2001, deve vigilare:

- sull'efficace attuazione del Modello, che consiste nel verificare la coerenza tra comportamenti concreti e Modello adottato;
- sull'adeguatezza del Modello, ossia l'idoneità dello stesso ad evitare i rischi di realizzazione degli illeciti di cui al D.Lgs. 231/2001;
- sull'aggiornamento del Modello, a seguito sia di mutamenti nella realtà organizzativa sia di eventuali mutamenti delle normative vigenti.

In particolare, al fine di consentire l'effettuazione di un'attività sistematica e formalizzata di monitoraggio delle anomalie, eccezioni e deroghe procedurali verificatesi nel periodo di riferimento, è previsto che sia messo a disposizione dell'Organismo di Vigilanza (odv@beltrame-group.com), a cura della Direzione IT:

- tempestivamente, ogni informazione relativa ad eventi che possano configurare uno dei reati presupposto di cui all'art. 24 *bis* del Decreto;
- trimestralmente, entro il mese successivo alla chiusura del periodo di monitoraggio, il Report segnalazione OdV D 13-10 "Esiti monitoraggio sul funzionamento dei controlli adottati".

7. ARCHIVIAZIONE

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nella presente procedura, comprese eventuali comunicazioni via e-mail, è conservata a cura della Direzione IT e messa a disposizione, su richiesta dell'Amministratore Delegato, del Consiglio di amministrazione, del Collegio Sindacale, della Società di Revisione, dell'Organismo di Vigilanza e dell'Internal Auditing.
I documenti prodotti nell'ambito delle attività descritte nel presente documento devono essere conservati per il periodo previsto dalle normative vigenti.

8. ALLEGATI

- D 13-10 – "Esiti monitoraggio sul funzionamento dei controlli adottati"