REGOLAMENTO AZIENDALE PER L'USO DEGLI STRUMENTI INFORMATICI E LA SICUREZZA ICT

1. INTRODUZIONE

1.1 Scopo e Destinatari

Questo Regolamento definisce le regole per l'utilizzo degli strumenti informatici e digitali aziendali, al fine di garantire la sicurezza delle informazioni e dei sistemi, la protezione dei dati e la tutela del patrimonio aziendale. Si applica a tutti coloro che utilizzano tali strumenti o accedono ai sistemi informativi dell'Azienda, inclusi dipendenti, collaboratori e terzi autorizzati. L'osservanza è obbligatoria.

1.2 Normativa di Riferimento

Il presente Regolamento è conforme al Regolamento (UE) 2016/679 (GDPR), alla Direttiva (UE) 2022/2555 (NIS2) e alla normativa nazionale applicabile (es. Legge 300/1970, Codice Civile).

1.3 Principi Generali

Gli strumenti forniti sono per uso lavorativo. L'utilizzo deve rispettare i principi di correttezza, diligenza, riservatezza e conformità alle policy aziendali. L'Azienda adotta un approccio basato sulla gestione del rischio e informa sulla possibile presenza di sistemi di tracciabilità e monitoraggio per finalità di sicurezza e tutela.

2. GESTIONE DELLA SICUREZZA ICT E RUOLI

2.1 Sistema di Sicurezza Aziendale

L'Azienda ha un sistema di sicurezza per la gestione delle informazioni, la protezione dei dati e la resilienza dei sistemi, basato su: identificazione asset, valutazione rischi, misure tecniche/organizzative, monitoraggio, gestione incidenti e continuità operativa.

2.2 Ruoli e Responsabilità

Sono stati definiti ruoli specifici per la gestione della sicurezza ICT e il rispetto della Direttiva NIS2, formalizzati nell'organigramma. Tutti i destinatari devono collaborare con il personale addetto alla sicurezza ICT e segnalare anomalie o incidenti.

- **Responsabile del Programma NIS2 (Ing. Mauro Piras):** Decide strategie e organizzazione della sicurezza.
- **Punto di Contatto ACN (Ing. Mauro Piras):** Gestisce le comunicazioni ufficiali con l'Agenzia per la Cybersicurezza Nazionale.
- **Responsabile Sicurezza Informatica (CISO) (Ing. Mauro Piras):** Sovrintende misure tecniche, monitoraggio e gestione vulnerabilità.

- **Responsabile Continuità Operativa (BCP/DR Manager) (Ing. Mauro Piras):** Gestisce piani di Business Continuity e Disaster Recovery.
- **Referente CSIRT Italia (Sig. Giacomo Corda):** Gestisce notifiche obbligatorie ad ACN in caso di incidente.
- **Responsabile Incidenti Informatici (Sig. Giacomo Corda):** Coordina le attività tecniche per la gestione degli incidenti.
- **Sostituto Punto di Contatto ACN (Sig. Giacomo Corda):** Subentra al Punto di Contatto principale in sua assenza.
- **Responsabile Sicurezza Fornitori (Sig. Mastio Angelo):** Monitora e gestisce la sicurezza nei rapporti con i fornitori tecnologici.
- **Sostituto Referente CSIRT Italia (Sig. Mastio Angelo):** Subentra al Referente CSIRT principale in sua assenza.

2.3 Formazione e Consapevolezza

L'Azienda promuove la formazione sulla sicurezza informatica e la protezione dei dati. La partecipazione è obbligatoria per ridurre il rischio di errore umano.

3. STRUMENTI AZIENDALI E CREDENZIALI

3.1 Assegnazione e Proprietà

Gli strumenti informatici, telematici ed elettronici sono di proprietà aziendale e forniti esclusivamente per lo svolgimento dell'attività professionale.

3.2 Obblighi di Custodia e Utilizzo

I destinatari devono usare gli strumenti solo per fini lavorativi (salvo usi personali minimi e tollerati), custodirli diligentemente, impedire accessi non autorizzati, non alterare configurazioni di sicurezza, non installare software non autorizzato e non disattivare sistemi di protezione.

3.3 Smarrimento, Furto o Danneggiamento

In caso di smarrimento, furto o danneggiamento, il destinatario deve comunicarlo immediatamente al responsabile o al Referente per la Sicurezza ICT, fornendo le informazioni necessarie per le misure tecniche (es. blocco account).

3.4 Restituzione degli Strumenti

Alla cessazione del rapporto o su richiesta, il destinatario deve restituire tutti gli strumenti, non trattenere copie di dati aziendali e collaborare alla disattivazione degli accessi.

3.5 Gestione Credenziali e Controllo Accessi

L'accesso ai sistemi è riservato ai soggetti autorizzati. Le credenziali (username, password, token) sono personali e non condivisibili. È vietato comunicarle a terzi, usare quelle altrui o lasciarle incustodite.

3.6 Requisiti delle Password e MFA

Le password devono rispettare i requisiti di sicurezza definiti dall'Azienda e, in particolare, devono avere una lunghezza adeguata, preferibilmente non inferiore a 10 caratteri, contenere una combinazione di lettere, numeri ed eventuali caratteri speciali, e non devono essere facilmente riconducibili al destinatario, all'Azienda o a informazioni di uso comune.

È vietato utilizzare password semplici, prevedibili, già utilizzate per altri servizi aziendali o personali, ovvero basate su nomi, date di nascita, riferimenti familiari o altre informazioni facilmente intuibili.

3.7 Compromissione Credenziali

In caso di sospetta compromissione, il destinatario deve cambiare subito la password, informare il responsabile o il Referente per la Sicurezza ICT e collaborare alle verifiche.

4. LOGGING E MONITORAGGIO

4.1 Sistemi di Registrazione (Log Tecnici)

I sistemi informativi aziendali generano registrazioni tecniche (log) relative a accessi e operazioni, per finalità di sicurezza informatica, protezione dati, tutela patrimonio, continuità operativa e gestione incidenti. Queste registrazioni non sono usate per il controllo sistematico dell'attività lavorativa.

4.2 Accesso ai Log e Conservazione

L'accesso ai log è consentito solo a soggetti autorizzati (es. Amministratore di Sistema, Referente per la Sicurezza ICT) per le finalità indicate. I dati sono conservati per un periodo proporzionato e poi cancellati o anonimizzati.

4.3 Controlli sugli Strumenti di Lavoro

L'Azienda può effettuare controlli sugli strumenti di lavoro assegnati nei limiti dell'art. 4 L. 300/1970. Tali controlli sono per esigenze organizzative/produttive, sicurezza o tutela del patrimonio. Le informazioni raccolte possono essere usate a fini disciplinari, rispettando la normativa e informando i lavoratori.

4.4 Verifiche Mirate e Indagini Difensive

In presenza di fondati elementi che facciano ragionevolmente presumere comportamenti illeciti, violazioni gravi degli obblighi contrattuali, utilizzi impropri degli strumenti aziendali o condotte idonee a arrecare danno all'Azienda, quest'ultima potrà effettuare verifiche mirate sugli strumenti assegnati al destinatario.

Tali verifiche saranno limitate ai soli dati e alle sole informazioni pertinenti rispetto ai fatti da accertare, saranno svolte nel rispetto dei principi di proporzionalità, pertinenza e minimizzazione e non avranno carattere generalizzato o continuativo.

Le verifiche sono finalizzate esclusivamente alla tutela dei diritti, della sicurezza, del patrimonio e dell'organizzazione aziendale e potranno essere effettuate anche ai fini della difesa dell'Azienda in sede disciplinare, civile o penale, nei limiti consentiti dalla normativa vigente.

4.5 Trasparenza e Informazione

Il presente Regolamento informa i destinatari sulla possibile esistenza di sistemi di registrazione e monitoraggio.

5. POSTA ELETTRONICA AZIENDALE

5.1 Tipologia e Principi di Utilizzo

L'Azienda assegna caselle di posta funzionali (per l'organizzazione) e nominative (per il lavoro individuale). L'uso deve rispettare correttezza, riservatezza, sicurezza e professionalità. È vietato l'uso per fini illeciti, l'invio di contenuti lesivi, la trasmissione di dati riservati a non autorizzati o l'iscrizione a servizi non pertinenti. Usi personali occasionali sono tollerati se non interferiscono con il lavoro o la sicurezza.

5.2 Archiviazione Comunicazioni

Le comunicazioni rilevanti devono essere archiviate nei sistemi condivisi e non solo nella casella personale, per garantire continuità e corretta gestione delle informazioni.

5.3 Misure di Sicurezza

La posta elettronica aziendale è soggetta a sistemi antivirus, antispam, protezione da phishing/malware e registrazioni tecniche. Il destinatario deve fare attenzione a email sospette, non comunicare credenziali via email non protetta e segnalare anomalie.

5.4 Accesso in Caso di Assenza

In caso di assenza prolungata o improvvisa, l'Azienda può attivare messaggi di risposta automatici o reindirizzare verso caselle funzionali. L'accesso alla casella nominativa avviene solo per esigenze organizzative o di sicurezza documentate, in modo proporzionato.

5.5 Cessazione del Rapporto

Alla cessazione del rapporto, se la casella è nominativa, la casella viene disattivata, mentre se è legata all'ufficio (non nominativa) viene trasferita al nuovo dipendente. Può essere attivato un messaggio automatico limitato. Non è consentita la consultazione generalizzata dell'archivio.

6. RETE INTERNET E SERVIZI CLOUD

6.1 Utilizzo Rete Internet

L'accesso alla rete internet aziendale è per uso lavorativo. È vietato accedere a siti illeciti, compromettere la sicurezza, scaricare materiale illecito o aggirare i sistemi di sicurezza.

6.2 Monitoraggio Traffico di Rete

L'Azienda può usare sistemi di protezione e monitoraggio (firewall, filtraggio, intrusion detection) per prevenire attacchi, proteggere dati/infrastrutture, tutelare il patrimonio e garantire continuità. Le registrazioni non sono per controllo sistematico dell'attività lavorativa.

6.3 Utilizzo Servizi Cloud

I servizi cloud per fini lavorativi devono essere usati solo tramite piattaforme autorizzate dall'Azienda. È vietato utilizzare account personali, profili browser personali o sistemi di archiviazione cloud personali per gestire attività, credenziali, documenti o informazioni aziendali.

In particolare, non è consentito salvare password aziendali su account personali del browser, sincronizzare dati di lavoro con profili personali o utilizzare servizi non autorizzati per la condivisione o conservazione di documenti aziendali.

L'utilizzo degli strumenti aziendali deve avvenire esclusivamente tramite account, profili e servizi approvati dall'Azienda, al fine di garantire la corretta separazione tra sfera personale e lavorativa, la sicurezza delle credenziali e la continuità operativa in caso di cessazione del rapporto o sostituzione del personale.

Salvo situazioni autorizzate in deroga a quanto riportato sopra per esigenze lavorative aziendali, con account personali utilizzati anche per attività lavorative.

6.4 Installazione Software e Download

L'installazione di software sui dispositivi aziendali è consentita solo previa autorizzazione. È vietato installare software non autorizzato, modificare configurazioni di sicurezza o disattivare antivirus. I download da internet devono provenire da fonti affidabili.

6.5 Protezione Dati durante la Navigazione

Il destinatario deve evitare la trasmissione di dati riservati su siti non protetti, verificare la sicurezza delle connessioni (HTTPS), non condividere informazioni aziendali tramite canali non autorizzati e segnalare anomalie/intrusioni.

7. LAVORO AGILE, ACCESSO REMOTO E DISPOSITIVI MOBILI

7.1 Principi Generali

L'accesso remoto ai sistemi e il lavoro agile sono consentiti rispettando le misure di sicurezza aziendali. Questo comporta rischi specifici che l'Azienda affronta con misure tecniche e la collaborazione dei destinatari.

7.2 Accesso Remoto

L'accesso remoto avviene tramite strumenti autorizzati (VPN, piattaforme cloud aziendali, MFA). È vietato accedere con strumenti non autorizzati. L'accesso remoto può essere soggetto a registrazioni tecniche per sicurezza.

7.3 Sicurezza Dispositivi Utilizzati

I dispositivi aziendali usati fuori sede devono essere protetti con credenziali personali, blocco schermo automatico, antivirus attivo, aggiornamenti di sicurezza e cifratura dati. È vietato disattivare o alterare le configurazioni di sicurezza. L'uso di dispositivi personali (BYOD) deve rispettare le misure aziendali.

7.4 Utilizzo Reti Esterne

Durante il lavoro da remoto, il destinatario deve evitare reti Wi-Fi pubbliche non protette, usare connessioni sicure (VPN), impedire a terzi l'accesso non autorizzato e non lasciare incustoditi dispositivi con dati aziendali.

7.5 Smarrimento, Furto o Compromissione

In caso di smarrimento, furto o sospetta compromissione di un dispositivo lavorativo, darne immediata comunicazione al responsabile o al Referente per la Sicurezza ICT per le misure tecniche necessarie (es. blocco account).

7.6 Protezione Informazioni Fuori Sede

Il destinatario deve non stampare documenti aziendali se non necessario, custodire documenti cartacei con diligenza, evitare discussioni di informazioni riservate in pubblico e garantire che persone non autorizzate non visualizzino lo schermo.

8. VIDEOSORVEGLIANZA E CONTROLLO ACCESSI FISICI

8.1 Finalità dei Sistemi

I sistemi di videosorveglianza sono installati solo per finalità legittime e determinate: sicurezza persone, protezione patrimonio, prevenzione illeciti, esigenze organizzative/sicurezza lavoro. Non sono usati per controllo sistematico dell'attività lavorativa e rispettano l'art. 4 L. 300/1970 e GDPR.

8.2 Installazione e Garanzie

L'installazione di impianti con potenziale controllo a distanza avviene previo accordo sindacale o autorizzazione dell'Ispettorato Territoriale del Lavoro. Le telecamere sono collocate per evitare riprese eccessive (es. aree riservate). Viene fornita adeguata informativa.

8.3 Conservazione Immagini

Le immagini sono conservate per un periodo limitato e proporzionato alle finalità, poi cancellate (salvo indagini o richieste autorità). L'accesso è solo per soggetti autorizzati.

8.4 Sistemi di Controllo Accessi Fisici (Badge)

Possono essere adottati sistemi di controllo accessi (badge) ai locali per: sicurezza locali/persone, gestione accessi aree riservate, prevenzione accessi non autorizzati. I dati degli accessi sono registrati per sicurezza e tutela patrimonio, non per controllo sistematico della prestazione lavorativa (salvo normativa).

8.5 Utilizzo delle Informazioni Raccolte

Le informazioni raccolte possono essere usate, nei limiti di legge, per sicurezza, tutela patrimonio, accertamento illeciti e fini disciplinari, garantendo liceità, proporzionalità, minimizzazione e trasparenza.

9. GESTIONE INCIDENTI INFORMATICI

9.1 Definizione di Incidente Informatico

Qualsiasi evento che comprometta o possa compromettere riservatezza, integrità, disponibilità o autenticità dei sistemi/dati aziendali (es. malware, phishing, accessi non autorizzati, furto dispositivi, cancellazione dati, malfunzionamenti, divulgazione non autorizzata).

9.2 Obbligo di Segnalazione Tempestiva

Chiunque venga a conoscenza di un incidente informatico deve informare immediatamente il proprio responsabile o il Referente per la Sicurezza ICT, fornire informazioni utili e collaborare alla gestione. La tempestività è essenziale.

9.3 Divieto di Interventi Non Autorizzati

In caso di incidente, è vietato tentare interventi tecnici autonomi, cancellare file/email sospette senza istruzioni, modificare configurazioni di sistema o disconnettere dispositivi senza istruzioni (salvo emergenza).

9.4 Attivazione Procedure Interne

In caso di segnalazione, l'Azienda attiva procedure interne per gestione incidenti, analisi tecnica, contenimento evento, valutazione data breach e notifiche alle autorità (se previste).

9.5 Collaborazione del Personale

Il destinatario deve collaborare attivamente con il personale incaricato della sicurezza informatica, fornendo informazioni e accesso ai dispositivi. Mancata segnalazione o occultamento possono comportare responsabilità disciplinari o legali.

10. DISMISSIONE E SMALTIMENTO APPARATI ELETTRONICI

10.1 Principi Generali

La dismissione di dispositivi informatici deve avvenire nel rispetto della sicurezza, riservatezza e protezione dei dati. Prima della cessione/smaltimento, l'Azienda adotta misure per la cancellazione sicura delle informazioni memorizzate, per prevenire accessi non autorizzati o usi illeciti.

10.2 Ambito di Applicazione

Si applica a computer, server, hard disk, smartphone, tablet, dispositivi USB, apparati di rete e altri dispositivi contenenti dati configurativi.

10.3 Cancellazione Sicura dei Dati

I dispositivi devono essere sottoposti a procedure di cancellazione sicura (software certificati, reset di fabbrica, distruzione fisica del supporto). In caso di danno, i supporti devono essere rimossi e distrutti.

10.4 Responsabilità e Autorizzazioni

Le operazioni di dismissione sono svolte solo da personale autorizzato o soggetti esterni incaricati. Il personale non è autorizzato a dismettere autonomamente, cedere a terzi o smaltire supporti senza autorizzazione.

10.5 Smaltimento RAEE

I dispositivi elettronici non più utilizzabili devono essere smaltiti secondo la normativa ambientale RAEE, tramite soggetti autorizzati.

10.6 Restituzione dei Dispositivi a Fine Rapporto

Alla cessazione del rapporto, il destinatario deve restituire tutti i dispositivi e supporti, non trattenere copie di dati aziendali e collaborare alle verifiche/cancellazioni.

11. VIOLAZIONI, RESPONSABILITÀ E REGIME DISCIPLINARE

11.1 Obbligo di Osservanza

Il rispetto del presente Regolamento è parte integrante degli obblighi contrattuali e professionali.

11.2 Violazioni del Regolamento

Costituiscono violazione (es. improprio uso strumenti, condivisione credenziali, trasmissione illecita dati, mancata segnalazione incidenti, alterazione sistemi sicurezza, installazione software non autorizzato, uso illecito rete/email, violazione misure sicurezza lavoro remoto). La gravità sarà valutata in base a circostanze, intenzionalità e conseguenze.

11.3 Conseguenze Disciplinari

Le violazioni possono comportare provvedimenti disciplinari, nel rispetto della normativa vigente, dell'art. 7 L. 300/1970, del CCNL e delle procedure interne. Possono includere sospensione o cessazione del rapporto di lavoro.

11.4 Responsabilità Civile e Penale

Comportamenti che causano danni all'Azienda o terzi possono comportare responsabilità civile e penale.

11.5 Revoca o Limitazione degli Accessi

In caso di violazioni o rischi informatici, l'Azienda può sospendere/limitare temporaneamente gli accessi o disattivare account/strumenti, anche in via cautelativa.

12. ENTRATA IN VIGORE, AGGIORNAMENTI E REVISIONI

12.1 Entrata in Vigore

Il Regolamento entra in vigore dalla data di adozione e viene diffuso ai destinatari. Con la presa visione, ci si impegna al rispetto.

12.2 Aggiornamenti e Modifiche

L'Azienda si riserva il diritto di modificare o integrare il Regolamento per adeguarlo a nuove normative, tecnologie, rafforzare la sicurezza, adattarsi all'evoluzione organizzativa o migliorare la gestione dei rischi. Le modifiche saranno comunicate.

12.3 Coordinamento con Altre Policy

Il Regolamento si integra con altre policy aziendali. In caso di contrasto, prevalgono le disposizioni normative vigenti e le policy specifiche.

12.4 Clausola di Salvaguardia

Qualora una o più disposizioni siano in contrasto con norme di legge sopravvenute, si intendono automaticamente sostituite dalle norme vigenti, restando valide le restanti disposizioni.