ADMIRAL Pay

Politica e Organizzazione per la sicurezza delle informazioni

ADMIRAL Pay Istituto di Pagamento S.r.l.
Tel. +39 06 526 239 800

infosec@novomatic.it
qualità@novomatic.it

https://www.admiralpay.it/

Iscrizione al Registro delle Imprese n. 04335420404

Rev. ottobre 2024

Politica e Organizzazione per la sicurezza delle informazioni

1 IL GRUPPO NOVOMATIC ITALIA

NOVOMATIC ITALIA S.p.A., fondata nel 2007, è la controllata Italiana della multinazionale Austriaca Novomatic AG, azienda leader nell'innovazione tecnologica degli apparecchi elettronici da intrattenimento e nella gestione di sale da gioco a livello mondiale ("**NOVOMATIC**" ovvero "NI"). Il gruppo **NOVOMATIC ITALIA** ("Gruppo Novomatic") opera sul territorio italiano come produttore, noleggiatore, distributore di apparecchi da intrattenimento e, tramite sue Società Controllate, come esercente e gestore di sale da gioco, nella raccolta del gioco nel comparto degli apparecchi, dell'on-line e delle scommesse sportive.

Sulla base dei principi promossi dalla Casa Madre, le Direzioni di **NOVOMATIC ITALIA S.p.A.**, **Admiral Gaming Network S.r.l.** (di seguito "**AGN**" o, congiuntamente, le "**Società**") e **Admiral Pay I.P. S.r.l.** (di seguito "**AP**" o, congiuntamente, le "**Società**") dichiarano di assicurare nel tempo l'applicazione del sistema di gestione della sicurezza delle informazioni per garantire la riservatezza, l'integrità e la disponibilità delle informazioni.

Le ragioni che hanno spinto le Società a tale atteggiamento sono:

- il mercato globale, che impone caratteristiche d'assoluta efficacia, pena la perdita di competitività, obiettivo conseguibile esclusivamente tramite un assetto organizzativo efficace;
- la capacità di affrontare rischi ed opportunità in relazione al contesto in cui si opera correlati agli obiettivi aziendali e alle aspettative delle parti interessate;
- il rispetto dei requisiti cogenti e degli impegni assunti con le parti interessate;
- la capacità di fornire con regolarità prodotti e servizi che soddisfino i requisiti dei clienti, aumentandone il livello di gradimento;
- la necessità di contrastare efficacemente le minacce di natura informatica e cyber;
- la necessità di garantire sul mercato un'immagine di affidabilità in termini di protezione del patrimonio informativo trattato e di misure di sicurezza adottate;
- l'esigenza della protezione dell'ambiente anche al fine di prevenire gli effetti del cambiamento climatico;
- la possibilità di rispondere con la certificazione di un Ente Terzo alle richieste dei Clienti, in merito al Sistema di Gestione della Sicurezza delle Informazioni del Gruppo NOVOMATIC;
- il mantenimento o potenziamento dell'attuale livello occupazionale perseguibile unicamente attraverso il costante miglioramento dello standard operativo Aziendale;
- la protezione delle informazioni in termini di riservatezza, l'integrità e la disponibilità delle stesse;
- il livello di protezione adeguato, coerenza, responsabilità collettiva, proporzionalità degli accessi e separazione dei compiti, difesa in profondità, security & privacy by design e minimizzazione delle informazioni, miglioramento continuo.

La gestione della sicurezza delle informazioni diviene conseguentemente obiettivo strategico del Gruppo NOVOMATIC.

2 OBIETTIVI DELLA POLITICA

Obiettivo del presente documento è quello di delineare i principi generali di sicurezza delle informazioni adottati dalle Società al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni ("**Sistema di Gestione**").
Tali principi sono concretizzati nella presente politica (di seguito "**Politica**") e declinati nel dettaglio nelle politiche e documenti del Sistema di Gestione che descrivono le direttive strategiche manageriali volte a indirizzare la gestione della sicurezza delle informazioni, le cui finalità sono la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione.
Tali obiettivi fanno riferimento alla necessità di contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, dell'integrità e della disponibilità delle informazioni aziendali considerate una risorsa di valore strategico per l'organizzazione, la cui tutela rappresenta una precisa responsabilità aziendale sancita anche a livello normativo.
In particolare:

- la tutela della riservatezza deve attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle informazioni, o la diffusione non controllata delle stesse;
- la tutela dell'integrità deve attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
- la tutela della disponibilità deve attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse in tempi utili al compimento della propria missione.

RISERVATEZZA
INTEGRITÀ
DISPONIBILITÀ

Tale tutela va perseguita al fine di mantenere un equilibrio costante nel tempo tra il livello di rischio operativo che l'azienda considera sopportabile e le necessarie misure di protezione, assicurando che la tutela delle informazioni e delle risorse informatiche si traduca anche nella salvaguardia dell'efficienza e dell'efficacia dei processi di erogazione dei servizi di business.
L'impossibilità di garantire alle informazioni aziendali una totale immunità dai rischi intrinseci alle procedure di gestione delle stesse piuttosto che a quelli derivanti dal tipo di strumento (cartaceo o informatico) utilizzato nell'ambito del trattamento, conduce alla necessità per le Società di dotarsi di un sistema di contromisure tale da non poter essere eluso se non intenzionalmente, e che consenta di contrastare adeguatamente tali rischi in termini di:

- prevenzione delle minacce e degli attacchi di natura informatica e cyber, onde ridurre al minimo la possibilità del verificarsi dei rischi di indisponibilità, accesso non autorizzato e perdita dell'integrità delle informazioni;
- reazione agli attacchi, onde evitarne, contenerne o minimizzarne i danni;
- ripristino della situazione antecedente al verificarsi del danno;
- investigazione per l'analisi e la valutazione dei danni subiti in seguito all'attacco.

La realizzazione e la conseguente gestione di tale sistema di governo della sicurezza delle informazioni, richiede l'indirizzamento di un insieme eterogeneo di interventi, di natura sia tecnologica che organizzativa, atti a garantire il raggiungimento e il mantenimento nel tempo dei livelli di sicurezza ritenuti adeguati.
L'insieme di tali interventi si configura come un processo continuo di identificazione, analisi e valutazione dei rischi, nonché di selezione delle migliori strategie di prevenzione e gestione degli stessi, volto a consentire il governo della sicurezza del Patrimonio Informativo aziendale.

Le Società, nel perseguire i propri obiettivi della sicurezza delle informazioni, ritengono prioritario l'impegno di tutto il personale; pertanto, mettono a disposizione risorse coerenti con gli obiettivi:

- l'organizzazione;
- le azioni e l'atteggiamento;
- le infrastrutture;
- il know how;
- le informazioni e dati;
- la sensibilizzazione, consapevolezza, formazione e capacità professionali delle persone e continuamente sviluppati.

3 AMBITO DI APPLICAZIONE

La Politica si applica a tutto il personale dipendente delle Società e a tutti i soggetti che collaborano a vario titolo. Si applica, inoltre, a tutti i processi e più in generale a tutte le risorse coinvolte nella gestione delle informazioni trattate dalle Società del Gruppo NOVOMATIC.
La Politica riguarda le modalità di gestione della sicurezza delle informazioni aziendali, nell'accezione più estesa del termine, utilizzate ai fini della loro elaborazione e custodia.

In particolare, le informazioni oggetto di protezione sono relative a:

- proprietà intellettuale;
- protezione dei dati personali;
- know how;
- business;
- informazioni contabili;
- informazioni sui dipendenti;
- informazioni su clienti, fornitori e partner.

Le risorse cartacee e informatiche, utilizzate per l'elaborazione e la custodia delle informazioni, cui sono indirizzati gli interventi di tutela comprendono:

- documenti contenenti le informazioni aziendali;
- siti aziendali e ambienti correlati (es. data center);
- piattaforme hardware;
- piattaforme software;
- infrastrutture di rete e di telecomunicazione;
- banche dati;
- documentazione tecnica;
- applicazioni gestionali e di business;
- supporti di memorizzazione per la conservazione dei dati.

Informazioni e risorse cartacee e informatiche, utilizzate per l'elaborazione e la custodia delle stesse, costituiscono le cosiddette risorse informative aziendali (di seguito "**Risorse Informative**"). Le Risorse Informative devono essere protette dal momento della loro creazione/introduzione in azienda, durante il loro utilizzo, fino al momento della distruzione/dismissione.
La responsabilità di proteggere le Risorse Informative in rapporto a eventi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzati, spetta all'utilizzatore delle stesse, ovvero al dipendente, nonché ai soggetti terzi (fornitori, consulenti, partner) con cui il Gruppo Novomatic intrattiene rapporti professionali.
Tale responsabilità discende dai principi di diligenza e correttezza, che devono indirizzare i comportamenti nell'ambito dello svolgimento delle attività lavorative.

4 TERMINI DI VALIDITÀ

La presente Politica assume validità dalla data di emissione (indicata in copertina). Ogni eventuale successivo aggiornamento del presente documento annulla e sostituisce, dalla data della sua emissione, tutte le versioni emesse precedentemente.

La Politica è sottoposta a revisione periodica, a cura della Funzione Group Quality & Health, Safety and Environment (di seguito "**Funzione Q&HSE**"), anche eventualmente su istanza di uno o più interessati, in caso di:

- eventi esterni (es. modifiche di carattere normativo); o
- eventi interni rilevanti, che abbiano impatto sulle attività definite nell'ambito della presente procedura.

5 RIFERIMENTI NORMATIVI E REGOLAMENTARI

- Standard Norma ISO 9001
- Standard Norma ISO/IEC 27001
- Standard Norma ISO 45001
- Standard Norma ISO 14001
- Standard Norma ISO/IEC 37001 – applicabile esclusivamente ad Admiral Pay IP S.r.l.
- Codice di Condotta di Novomatic AG;
- Codice Etico del Gruppo NOVOMATIC Italia;
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 ove adottato dalle Società del Gruppo NOVOMATIC Italia;
- D. Lgs. 231/2001 recante disposizioni in materia di "Responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica";
- Regolamento UE 679/2016 (GDPR - General Data Protection Regulation);

- D.lgs. 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" e s.m.i;
- Policy, Linee Guida, Procedure del Gruppo NOVOMATIC e di NOVOMATIC AG;
- D.Lgs. 9 aprile 2008, n. 81, e s.m.i. in materia di tutela della salute e della sicurezza nei luoghi di lavoro
- Normative, direttive e regolamenti specifici di settore

EFFICIENZA
ATTENZIONE
CONFORMITÀ

6 REQUISITI DI CONFORMITÀ

La conformità ai requisiti di sicurezza definiti dalle normative cogenti, dagli standard e dalle best practice, individuati dal Gruppo Novomatic, risulta imprescindibile nell'ambito del raggiungimento degli obiettivi espressi all'interno della Politica della Sicurezza delle Informazioni.
Tali requisiti sono presi in considerazione nell'ambito della definizione degli obiettivi di sicurezza aziendali e formalizzati all'interno di direttive strategiche che indirizzano la tutela delle risorse informative aziendali.
Tutte le attività delle Società devono essere svolte nell'osservanza della legge, in un quadro di concorrenza leale per creare valore con integrità, per i propri clienti, i collaboratori e la collettività.
Creare valore con integrità vuol dire agire con onestà, correttezza e buona fede, nel rispetto degli interessi legittimi dei clienti, dei dipendenti, dei partner commerciali e finanziari e delle collettività con cui le società si relazionano.

Nell'ambito della definizione delle strategie di gestione della sicurezza delle informazioni, le Società si pongono l'obiettivo di ottemperare ai requisiti derivanti dai principi generali enunciati dall'attuale legislazione italiana in materia di:

- criminalità informatica;
- protezione dei dati personali;
- tutela del software e delle banche dati;
- validità giuridica del documento informatico, della firma digitale e della firma elettronica;
- internet.

Le Società, nell'ambito della definizione delle strategie di gestione della sicurezza delle informazioni, si pongono l'obiettivo di ottemperare anche ai requisiti derivanti dalle normative specifiche applicabili ai servizi di business erogato sulla concessione di AGN per l'attivazione e la conduzione operativa della rete per la gestione telematica del gioco lecito mediante apparecchi da divertimento e intrattenimento nonché delle attività e funzioni connesse.
Le Società nell'ambito della gestione aziendale sono inoltre tenute al rispetto della normativa cogente e interna applicabile.

Le Società si pongono come obiettivo l'adozione di un approccio metodologico alla gestione delle problematiche inerenti alla sicurezza delle informazioni conforme agli standard ed alle best practice, nazionali e internazionali, di riferimento per la definizione di ruoli, responsabilità, procedure formali (sia per l'operatività aziendale che per la trattazione delle emergenze) di gestione dei processi legati alla sicurezza - inclusa la norma ISO/IEC 27001:2022 e le norme correlate.

7 DIRETTIVE STRATEGICHE E PRINCIPALI OBIETTIVI

I principi generali cui le Società si ispirano nella gestione della sicurezza delle informazioni sono articolati nelle seguenti tematiche:

- identificazione, classificazione e gestione delle informazioni;
- norme comportamentali per la gestione sicura delle risorse informative;
- gestione del personale;
- aspetti contrattuali connessi alla sicurezza delle informazioni;
- gestione della sicurezza fisica;
- gestione sicura degli accessi logici;
- gestione sicura dei sistemi e dei servizi;
- gestione degli eventi anomali e degli incidenti;
- gestione della business continuity;
- monitoraggio, tracciamento e verifiche tecniche;
- rispetto della normativa.

L'instaurazione, l'applicazione, il mantenimento e il miglioramento del Sistema di Gestione della Sicurezza delle Informazioni, in accordo alla norma ISO/IEC 27001:2022 si propone attraverso la propria politica, i seguenti obiettivi:

- raggiungere la posizione di leader nazionale sul mercato;
- garantire sul mercato un'immagine di affidabilità in termini di protezione del patrimonio informativo trattato e di misure di sicurezza adottate;
- migliorare continuamente l'efficienza complessiva dell'organizzazione e del sistema di gestione della sicurezza delle informazioni, assicurando la promozione al proprio interno del rigoroso rispetto di tutte le regole organizzative e procedurali adottate dal Gruppo Novomatic;
- assicurare il rispetto delle leggi e norme applicabili e degli impegni contrattuali, obblighi di conformità ed accordi con le parti interessate, nonché dei principi di onestà, trasparenza, lealtà e correttezza;
- individuare, monitorare e migliorare continuamente le proprie attività per garantire la riservatezza, integrità e disponibilità, e prevenire o ridurre i rischi di natura fisica, logica e organizzativa;
- incoraggiare e favorire l'attenzione, la consapevolezza e la sensibilizzazione e le competenze in materia di sicurezza delle informazioni;
- perseguire attraverso le politiche, strumenti e controlli la tutela dei dati personali dei propri dipendenti, dei clienti e delle parti interessate;
- perseguire attraverso le politiche, strumenti e controlli la tutela dei sistemi informatici, la

tutela dell'immagine aziendale, la protezione dei dati personali, la prevenzione delle frodi e la tutela del copyright;

- aumentare, nel proprio personale, e nei fornitori esterni, il livello di consapevolezza e la cultura sulla sicurezza delle informazioni, anche al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o accidentali;
- individuare, monitorare e migliorare continuamente le proprie attività in ottica di riduzione dei rischi e individuazione delle opportunità in coerenza con le strategie di business, tutelando i diritti e le libertà delle persone fisiche;
- migliorare l'infrastruttura tecnologica e l'organizzazione al fine di incrementare la ridondanza e assicurare la continuità operativa dei servizi e delle informazioni;
- creare valore aggiunto, attraverso il perseguimento di migliori condizioni economiche, sociali e professionali, nell'ambito della propria specifica attività istituzionale.

8 CICLO DI VITA DELLA POLITICA E RESPONSABILITÀ

La Politica viene rivista almeno annualmente in occasione del riesame del Sistema di Gestione della Sicurezza delle Informazioni, definendo obiettivi e traguardi specifici, considerando l'evoluzione del contesto aziendale e l'analisi dei potenziali rischi sulle informazioni, e se del caso, riemessa.

Essa è approvata, in conformità a quanto previsto dalle Linee Guida di Gruppo sulla produzione normativa aziendale, dal Consiglio di Amministrazione di Novomatic che, con il supporto del Rappresentante della Direzione, ha l'autorità e responsabilità di attuare e mantenere il controllo dell'applicazione e dell'efficacia del Sistema di Gestione.
La Politica integrata viene diffusa mediante il portale aziendale ed è disponibile ai fornitori ed alle parti interessate tramite il sito istituzionale.

POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI - LIFECYCLE

ADMIRALPay