

NOVOMATIC
ITALIA

Politica e Organizzazione per la sicurezza delle informazioni

NOVOMATIC ITALIA S.p.A.
Tel. +39 06 526 239 01

infosec@novomatic.it
qualità@novomatic.it

www.novomatic.it

Iscrizione al Registro delle Imprese n. 03677960407

Rev. novembre 2026



Politica e Organizzazione per la sicurezza delle informazioni



SOMMARIO

1. IL GRUPPO NOVOMATIC ITALIA
2. OBIETTIVI
3. CAMPO DI APPLICAZIONE
3.1 SOCIETÀ INDIVIDUATE QUALI SOGGETTI NIS2
3.2 SOCIETÀ IN PERIMETRO DORA
4. TERMINI DI VALIDITÀ
5. RIFERIMENTI NORMATIVI E REGOLAMENTARI
6. REQUISITI DI CONFORMITÀ
7. DIRETTIVE STRATEGICHE, PRINCIPI DI SICUREZZA E FINALITÀ
8. POLITICA DI SICUREZZA DEI SISTEMI INFORMATIVI E DI RETE
9. ORGANIZZAZIONE DELLA SICUREZZA INFORMATICA
9.1 RESPONSABILITÀ DEGLI ORGANI DI AMMINISTRAZIONE
10. CICLO DI VITA DELLA POLITICA E RESPONSABILITÀ
11. ADOZIONE DELLA POLITICA
12. MONITORAGGIO E REVISIONE DELLA POLITICA

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 (di seguito 'Novomatic' ovvero 'NI').
Il gruppo NOVOMATIC ITALIA (di seguito, singolarmente, le "Società" ovvero, nel complesso, il "Gruppo NOVOMATIC" o "Gruppo") 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, nonché come gestore per l'esercizio e la raccolta a distanza dei giochi pubblici ed erogazione di servizi per pagamenti elettronici e servizi al cittadino.

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'),**
- **HBG On Line Gaming S.r.l. (di seguito 'HBG' o, congiuntamente, le 'Società'),**
- **Admiral Pay I.P. S.r.l. (di seguito 'AP', 'Admiral Pay' 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 Società hanno adottato tale approccio alla luce dei seguenti fattori strategici e operativi, ritenuti essenziali per assicurare un assetto organizzativo solido ed efficiente e sostenere nel tempo l'efficacia e la competitività del Gruppo:

- la capacità di individuare, valutare e gestire rischi e opportunità correlati al contesto in cui operano, agli obiettivi aziendali e alle aspettative delle parti interessate;
- il rispetto degli obblighi normativi applicabili e degli impegni assunti nei confronti delle parti interessate;
- la capacità di fornire in modo continuativo prodotti e servizi conformi ai requisiti della clientela, contribuendo al miglioramento della sua soddisfazione;
- l'esigenza di garantire e consolidare sul mercato un'immagine di affidabilità, assicurando un adeguato livello di protezione del patrimonio informativo e l'adozione di idonee misure di sicurezza;
- l'impegno alla tutela dell'ambiente, anche attraverso iniziative finalizzate alla prevenzione e mitigazione degli effetti del cambiamento climatico;
- la possibilità di rispondere alle richieste della clientela attraverso la certificazione del Sistema di Gestione della Sicurezza delle Informazioni rilasciata da un organismo indipendente;
- il mantenimento e lo sviluppo dei livelli occupazionali, perseguibili attraverso il miglioramento continuo dell'efficacia e dell'efficienza dei processi aziendali;
- la protezione delle informazioni sotto i profili della riservatezza, integrità e disponibilità;
- la necessità di prevenire e contrastare efficacemente le minacce di natura informatica e cyber;
- l'applicazione dei principi di adeguatezza e proporzionalità delle misure di sicurezza, di responsabilità condivisa, di segregazione dei compiti, di difesa in profondità, di security e privacy by design, di minimizzazione delle informazioni e di miglioramento continuo.

In tale contesto la gestione della sicurezza delle informazioni, dei sistemi informativi e di rete rappresenta un obiettivo strategico e un elemento essenziale della governance aziendale del Gruppo NOVOMATIC, a supporto della continuità operativa, della resilienza cyber, della conformità normativa e della tutela degli interessi delle parti interessate.
La presente politica (di seguito "Politica") è attuata attraverso il corpus documentale del Sistema di Gestione della Sicurezza delle Informazioni, costituito, tra l'altro, da politiche tematiche, procedure operative, piani, standard, registri e controlli.



2 OBIETTIVI DELLA POLITICA

Obiettivo del presente documento è quello di delineare i principi generali di sicurezza delle informazioni adottati dalle Società per istituire, attuare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni efficiente e sicuro ("**Sistema di Gestione**"). Tali principi sono formalizzati nella presente Politica e trovano ulteriore declinazione nelle politiche, procedure e negli altri documenti del Sistema di Gestione, che definiscono gli indirizzi strategici e operativi e descrivono le direttive manageriali volte a garantire la protezione dei dati e delle risorse del sistema informativo utilizzate per il loro trattamento, nonché a definire le relative responsabilità di gestione.

Tali obiettivi di sicurezza delle informazioni fanno riferimento alla necessità di contenere, entro limiti accettabili, il rischio di compromissione della riservatezza, dell'integrità e della disponibilità delle informazioni aziendali considerate un patrimonio strategico per le Società, la cui tutela rappresenta una precisa responsabilità organizzativa aziendale sancita anche a livello normativo e un obbligo di conformità ai requisiti normativi applicabili.
In particolare, le Società perseguono i seguenti principi fondamentali:

- riservatezza: prevenire accessi non autorizzati, divulgazioni improprie o utilizzi non autorizzati delle informazioni. 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;
- integrità: garantire la completezza, l'accuratezza e la protezione delle informazioni da modifiche o alterazioni non autorizzate, o il danneggiamento del formato fisico e/o del contenuto semantico. 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;

RISERVATEZZA
INTEGRITÀ
DISPONIBILITÀ

- disponibilità: assicurare che le informazioni, i sistemi e le risorse siano accessibili ai soggetti autorizzati nei tempi necessari allo svolgimento delle attività aziendali.

La tutela della disponibilità deve attuarsi mediante interventi idonei a garantire l'accesso alle risorse, nei tempi utili al compimento delle attività previste, esclusivamente al personale autorizzato. La tutela delle informazioni è perseguita mediante un approccio equilibrato e proporzionato al rischio, volto a garantire nel tempo un adeguato livello di protezione del patrimonio informativo e delle risorse informatiche e di rete, salvaguardando al contempo l'efficienza e l'efficacia dei processi aziendali e dei servizi di business. Considerata l'impossibilità di eliminare completamente i rischi associati alla gestione delle informazioni, indipendentemente dal supporto utilizzato, cartaceo o digitale, le Società adottano un sistema integrato di misure organizzative, procedurali e tecnologiche finalizzato a:

- prevenire e ridurre i rischi di riservatezza, integrità e disponibilità delle informazioni, derivanti da minacce e attacchi di natura informatica e cyber;
- rilevare, gestire e contenere gli effetti di eventi di sicurezza e incidenti;
- ripristinare tempestivamente le condizioni operative e di sicurezza precedenti all'evento;
- analizzare e valutare gli impatti degli incidenti al fine di individuare adeguate azioni correttive e di miglioramento.

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 riconoscono inoltre che il conseguimento degli obiettivi di sicurezza richiede il coinvolgimento e l'impegno di tutto il personale e, a tal fine, assicurano la disponibilità di risorse adeguate in termini di:

- organizzazione e processi;
- azioni e atteggiamento;
- infrastrutture e tecnologie;
- competenze e know-how;
- informazioni e dati;
- sensibilizzazione, consapevolezza, formazione, e capacità professionali del personale.



3 CAMPO DI APPLICAZIONE

Tipo di documento	Documento di Sistema Integrato	
Applicazione/Sistema di Gestione	Novomatic Italia S.p.A.	ISO 9001, ISO 27001, ISO 14001, ISO4 5001, PdR 125
	Admiral Gaming Network S.r.l.	ISO 9001, ISO 27001, ISO14001, ISO 45001
	Admiral Pay IP S.r.l.	ISO 9001, ISO 27001, ISO 37001
	HBG On Line Gaming S.r.l.	ISO 9001, ISO 27001, ISO 45001, ISO 50001, ISO 14001, ISO 26000
Circolazione Il presente documento viene inserito nella raccolta della normativa aziendale pubblicata sulla intranet aziendale.		

La presente Politica si applica a tutto il personale delle Società, nonché alle persone che collaborano con esse e alle terze parti che, a qualsiasi titolo, trattano informazioni o utilizzano risorse aziendali per conto del Gruppo NOVOMATIC.

Essa disciplina la sicurezza delle informazioni e si estende a tutti i processi, le attività e gli asset coinvolti nella loro elaborazione, conservazione, trasmissione e protezione.

Sono oggetto di tutela tutte le informazioni aziendali, comprese la proprietà intellettuale, i dati personali, il know-how, le informazioni di business, contabili e finanziarie, quelle relative al personale, nonché le informazioni riguardanti clienti, fornitori e partner.

La protezione si applica altresì a tutte le risorse fisiche e digitali utilizzate per la gestione delle informazioni, incluse documentazione e archivi, siti e ambienti tecnologici, piattaforme hardware e software, infrastrutture di rete e telecomunicazione, banche dati, documentazione tecnica, applicazioni gestionali e supporti di memorizzazione.

Le informazioni e le risorse utilizzate per la loro elaborazione, conservazione e trasmissione costituiscono le risorse informative del Gruppo e devono essere adeguatamente protette durante l'intero ciclo di vita, dalla creazione o acquisizione fino alla conservazione, utilizzo e successiva dismissione o distruzione.

La protezione delle risorse informative da eventi accidentali o intenzionali che possano comprometterne la riservatezza, l'integrità o la disponibilità è responsabilità di chiunque ne faccia uso, sia all'interno delle Società sia nell'ambito dei rapporti con fornitori, consulenti, partner e altri soggetti terzi. Tale responsabilità trova fondamento nei principi di diligenza, correttezza e responsabilizzazione che devono orientare i comportamenti nello svolgimento delle attività lavorative.

3.1 Società individuate quali soggetti NIS2

Per ciascuna Società soggetta al D.lgs. 138/2024 - Recepimento della Direttiva (UE) 2022/2555 (NIS2):

- è definito e mantenuto aggiornato il perimetro NIS, comprendente i servizi e le attività rilevanti, i sistemi informativi e di rete che li supportano, gli asset, le relative dipendenze e i soggetti e fornitori coinvolti;
- è mantenuta una matrice di conformità che associa i requisiti NIS2, del D.lgs. 138/2024 e delle specifiche di base ACN applicabili ai relativi documenti, controlli, responsabili ed evidenze di attuazione, nonché agli eventuali scostamenti, misure compensative e piani di adeguamento.
- Le misure di sicurezza previste dalla presente Politica sono declinate, per ciascun soggetto NIS, nelle specifiche di base applicabili definite dall'ACN e sono oggetto di apposito assessment di conformità e di piano di adeguamento.

3.2 Società in perimetro DORA

Per Admiral Pay, soggetta al Regolamento (UE) 2022/2554 (DORA) in quanto Istituto di Pagamento, è definito e mantenuto aggiornato il perimetro DORA ed è assicurata, mediante apposita matrice di conformità, la tracciabilità dei requisiti applicabili rispetto a controlli, responsabilità ed evidenze, nonché agli eventuali scostamenti e piani di adeguamento, nell'ambito del quadro per la gestione dei rischi ICT.

DORA costituisce lex specialis rispetto alla disciplina NIS2 in materia di gestione dei rischi ICT e di segnalazione degli incidenti, conformemente all'art. 4 della Direttiva (UE) 2022/2555 e al considerando 16 del Regolamento (UE) 2022/2554.

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 riesaminata con cadenza almeno biennale a cura delle Funzioni ISO Certifications, Cybersecurity e Governance & Awareness, anche su richiesta di una o più parti interessate e, comunque, senza ingiustificato ritardo in caso di incidenti significativi o di modifiche organizzative, normative, tecnologiche o del profilo di rischio che ne rendano necessario l'aggiornamento. In particolare, la Politica è sottoposta a revisione in caso di:
- eventi esterni (es. modifiche di carattere normativo e regolamentare, ecc.);
- eventi interni rilevanti (es. modifiche delle politiche aziendali, variazioni della struttura organizzativa, nuovi modelli di business, ecc.), che abbiano impatto sulle attività definite nell'ambito della presente Politica.



5 RIFERIMENTI NORMATIVI E REGOLAMENTARI

- 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;
- D.Lgs. 1° settembre 1993, n. 385 e s.m.i. – Testo unico delle leggi in materia bancaria e creditizia, – applicabile ad Admiral Pay I.P. S.r.l;
- D.Lgs. 27 gennaio 2010, n. 11 e s.m.i. – Attuazione della disciplina europea relativa dei servizi di pagamento nel mercato interno – applicabile ad Admiral Pay I.P. S.r.l.;



- Disposizioni di vigilanza della Banca d'Italia per gli istituti di pagamento e gli istituti di moneta elettronica, emanate il 17 maggio 2016 e s.m.i, – applicabile ad Admiral Pay I.P. S.r.l.;
- Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (DORA), e relativi atti delegati e di esecuzione – applicabile ad Admiral Pay I.P. S.r.l.;
- D.Lgs. 10 marzo 2025, n. 23 – Adeguamento della normativa nazionale al Regolamento (UE) 2022/2554 e recepimento della Direttiva (UE) 2022/2556 in materia di resilienza operativa digitale per il settore finanziario – applicabile ad Admiral Pay I.P. S.r.l.;
- Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS 2);
- D.Lgs. 4 settembre 2024, n. 138 – Recepimento della Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS 2);
- Determinazione ACN n. 379907/2025 e relativi Allegati 1 e 2, recanti le misure di sicurezza di base rispettivamente per i soggetti essenziali e per i soggetti importanti;
- Policy, Linee Guida, Procedure del Gruppo NOVOMATIC Italia e di NOVOMATIC AG.

EFFICIENZA
ATTENZIONE
CONFORMITÀ



6 REQUISITI DI CONFORMITÀ

La conformità ai requisiti di sicurezza definiti dalla normativa e dai regolamenti applicabili, nonché agli standard e alle buone pratiche di riferimento adottati dal Gruppo NOVOMATIC, costituisce un presupposto essenziale e imprescindibile per il raggiungimento degli obiettivi di sicurezza delle informazioni definiti dalla presente Politica.

Tali requisiti sono considerati nella definizione degli obiettivi di sicurezza, delle misure di protezione e delle direttive strategiche che disciplinano la tutela delle risorse informative aziendali.

Tutte le attività svolte dalle Società devono essere condotte nel pieno rispetto delle disposizioni normative applicabili e dei principi di leale concorrenza, perseguendo la creazione di valore sostenibile per la clientela, il personale, i/le collaboratori/collaboratrici e la collettività.

La creazione di valore si fonda sull'integrità, intesa come l'adozione di comportamenti improntati a onestà, correttezza, trasparenza e buona fede, nel rispetto dei legittimi interessi della clientela, del personale, delle organizzazioni partner in ambito commerciale e finanziario e delle comunità con cui le Società interagiscono.

Nell'ambito della gestione della sicurezza delle informazioni, le Società perseguono la conformità alla legislazione applicabile, con particolare riferimento alla criminalità informatica, alla protezione dei dati personali, alla tutela del software e delle banche dati, alla validità giuridica dei documenti informatici e delle firme elettroniche, nonché all'utilizzo delle tecnologie e dei servizi digitali.

Nell'ambito della definizione delle strategie, le Società perseguono la conformità ai requisiti normativi e regolamentari applicabili ai rispettivi ambiti di attività e alle relative concessioni, autorizzazioni e servizi erogati, inclusi:

- i servizi digitali, informatici e di sicurezza erogati da Novomatic, in qualità di capogruppo, a supporto delle società del Gruppo;
- i servizi e le attività svolte da AGN nell'ambito della gestione telematica del gioco lecito mediante apparecchi da divertimento e intrattenimento nonché delle attività e funzioni connesse;
- i servizi e le attività svolte da HBG nell'ambito dell'esercizio e della raccolta a distanza dei giochi pubblici;
- i servizi di pagamento prestati da Admiral Pay, nonché la gestione dei relativi sistemi informativi, nel rispetto della normativa di settore applicabile e dei requisiti di resilienza operativa digitale.

Le Società sono inoltre tenute al rispetto della normativa cogente interna applicabile.

A tal fine, adottano un approccio strutturato alla gestione della sicurezza delle informazioni, coerente

con gli standard e le buone pratiche nazionali e internazionali di riferimento, inclusa la norma UNI CEI EN ISO/IEC 27001:2024 e le relative norme correlate.
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 PRINCIPI DI SICUREZZA E FINALITÀ

I principi di gestione della sicurezza delle informazioni adottati dalle Società si applicano all'insieme dei processi, delle attività e delle risorse informative del Gruppo e trovano attuazione nelle seguenti aree:

- classificazione e gestione delle informazioni;
- utilizzo sicuro delle risorse informative;
- gestione del personale e delle responsabilità in materia di sicurezza;
- gestione dei rapporti contrattuali con clienti, fornitori e partner;
- sicurezza fisica e ambientale;
- gestione degli accessi e delle identità digitali;
- sicurezza dei sistemi, delle reti e dei servizi;
- gestione degli eventi di sicurezza e degli incidenti;
- continuità operativa e resilienza dei servizi;
- monitoraggio, tracciamento e verifica delle misure di sicurezza;
- gestione della conformità ai requisiti applicabili.

Attraverso il Sistema di Gestione, sviluppato in coerenza con la norma UNI CEI EN ISO/IEC 27001:2024 e con le altre normative e standard applicabili, le Società perseguono le seguenti finalità:

- consolidare la posizione competitiva e la reputazione del Gruppo attraverso un'elevata affidabilità nella gestione delle informazioni e dei servizi;
- migliorare continuamente l'efficacia del Sistema di Gestione e dei processi organizzativi;
- garantire il rispetto degli obblighi normativi, regolamentari, contrattuali e degli impegni assunti verso le parti interessate;
- proteggere il patrimonio informativo e i sistemi aziendali assicurandone riservatezza, integrità, disponibilità e resilienza;
- tutelare i dati personali, i diritti e le libertà degli interessati attraverso adeguate politiche, controlli e misure di sicurezza;
- sviluppare la cultura della sicurezza e accrescere la consapevolezza del personale, dei/delle collaboratori/collaboratrici e delle organizzazioni fornitrici;
- rafforzare l'infrastruttura tecnologica e organizzativa per garantire continuità operativa, capacità di risposta agli incidenti e resilienza dei servizi;
- creare valore sostenibile per le parti interessate attraverso il miglioramento delle condizioni economiche, sociali e professionali connesse alle attività del Gruppo.

8 POLITICA DI SICUREZZA
DEI SISTEMI INFORMATIVI E DI RETE

La presente Politica ricomprende definisce la politica di sicurezza dei sistemi informativi e di rete che delinea gli indirizzi adottati dalle Società per proteggere sistemi informativi, infrastrutture di rete, servizi digitali e relativi dati da eventi accidentali o intenzionali che possano comprometterne riservatezza, integrità, disponibilità, autenticità e resilienza.
Essa si applica all'intero ciclo di vita dei sistemi e dei servizi, inclusi quelli affidati a organizzazioni fornitrici, secondo un approccio basato sul rischio e proporzionato alla criticità degli asset e dei processi supportati.
L'analisi e la gestione del rischio sono condotte secondo la "Metodologia di Analisi e Gestione del Rischio per la Sicurezza delle Informazioni" adottata dalle Società, tenendo conto dei requisiti applicabili, degli standard di riferimento e delle informazioni derivanti dall'esercizio, incluse vulnerabilità, eventi e incidenti di sicurezza. La metodologia disciplina l'identificazione, la valutazione e il trattamento dei rischi e dei relativi controlli, l'accettazione del rischio residuo, nonché il monitoraggio, la comunicazione e il riesame periodico del profilo di rischio.
Gli organi di amministrazione definiscono e approvano, nell'ambito del risk appetite framework aziendale, i livelli di tolleranza al rischio ICT e agli impatti derivanti dall'interruzione dei servizi ICT, assicurandone la coerenza con la strategia aziendale, la criticità delle funzioni supportate e gli obiettivi di resilienza operativa digitale.
Per Admiral Pay è inoltre definita e mantenuta una strategia di resilienza operativa digitale, integrata nel framework di gestione del rischio ICT e coerente con la strategia aziendale e il risk appetite. La Strategia definisce i livelli di tolleranza e gli obiettivi di sicurezza e resilienza, i relativi indicatori, l'architettura ICT di riferimento e i presidi di prevenzione, rilevazione, risposta, recupero, testing e comunicazione in caso di incidenti ICT.
Gli esiti del monitoraggio, degli audit, delle verifiche e dei test di sicurezza, degli incidenti, delle esercitazioni e delle valutazioni del rischio sono utilizzati per aggiornare il profilo di rischio, definire le azioni correttive e gli eventuali interventi di adeguamento, nonché migliorare le misure di sicurezza.
Sono definiti e mantenuti indicatori e metriche di sicurezza e resilienza, inclusi, ove applicabili, Key Risk Indicators (KRI), Key Performance Indicators (KPI), al fine di monitorare l'efficacia delle misure e il livello di maturità della sicurezza.



Sulla base del profilo di rischio risultante e in coerenza con il Sistema di Gestione, con il perimetro NIS2, DORA e con gli altri requisiti normativi e regolamentari applicabili a ciascuna Società, sono adottate e documentate politiche, procedure e altre disposizioni attuative relative almeno a:

1. gestione del rischio;
2. ruoli e alle responsabilità;
3. affidabilità delle risorse umane;
4. conformità e agli audit di sicurezza;
5. sicurezza della catena di approvvigionamento;
6. gestione degli asset e delle vulnerabilità;
7. risposta agli incidenti e al ripristino;
8. continuità operativa, al ripristino in caso di disastro e alla gestione delle crisi;
9. autenticazione, gestione identità digitali e controllo degli accessi;
10. sicurezza dei dati e alla crittografia;
11. sviluppo software, alla configurazione, alla manutenzione e alla dismissione sicuri dei sistemi;
12. change management;
13. protezione delle reti e delle comunicazioni;
14. monitoraggio degli eventi;
15. sicurezza fisica;
16. formazione e alla consapevolezza.



In questo ambito assumono particolare rilevanza le seguenti aree:

- **sicurezza della Catena di approvvigionamento** (5): le Società gestiscono i rischi della catena di approvvigionamento attraverso la valutazione e il monitoraggio dei fornitori e delle terze parti, includendo almeno i fornitori ICT rilevanti e le forniture con potenziali impatti sulla sicurezza dei sistemi informativi e di rete, nonché mediante l'adozione di adeguati requisiti di sicurezza e obblighi contrattuali.
- **gestione degli asset e delle vulnerabilità** (6): le Società adottano un processo formalizzato di gestione delle vulnerabilità che ne disciplina l'identificazione, la classificazione, la prioritizzazione, il trattamento, la verifica della risoluzione e la gestione delle eventuali eccezioni, secondo criteri basati sul rischio e sulla criticità degli asset. Ove applicabile, il processo include la divulgazione coordinata delle vulnerabilità in conformità alla normativa vigente.
- **gestione incidenti di sicurezza** (7): le Società assicurano la gestione degli incidenti di sicurezza informatica attraverso un processo formalizzato che disciplina classificazione, valutazione, escalation, comunicazione e notificazione degli incidenti, nel rispetto degli obblighi e delle tempistiche previsti dalla normativa NIS2, DORA e dalle relative disposizioni attuative, ove applicabili.

- **gestione della continuità operativa** (8): le Società assicurano la continuità operativa, la resilienza e la gestione delle crisi mediante l'identificazione delle funzioni e dei servizi critici, la definizione dei requisiti di continuità e ripristino (RTO e RPO), l'adozione di piani di continuità operativa e disaster recovery, nonché lo svolgimento di periodici test, esercitazioni e riesami. Le attività comprendono la gestione dei backup e del ripristino di informazioni e sistemi attraverso procedure formalizzate, adeguate misure di protezione delle copie di backup e verifiche periodiche dell'effettiva capacità di ripristino. Per Admiral Pay, la definizione dei requisiti di continuità e ripristino è supportata da una Business Impact Analysis (BIA) documentata, periodicamente aggiornata, che considera la criticità delle funzioni e dei servizi, le dipendenze ICT e da fornitori terzi, le interdipendenze tra asset e processi, gli impatti quantitativi e qualitativi delle interruzioni e i requisiti di ridondanza.
- **gestione degli accessi logici** (9): le Società adottano meccanismi di autenticazione forte e multi-fattore, proporzionati al rischio e alla criticità dei sistemi e dei servizi, e disciplinano la gestione degli account privilegiati e amministrativi secondo i principi di minimo privilegio, segregazione dei compiti, tracciabilità e revisione periodica degli accessi.
- **sicurezza dei dati** (10): le Società assicurano l'adozione e la gestione di meccanismi crittografici adeguati alla classificazione delle informazioni, alla criticità dei sistemi e ai rischi associati, inclusa la gestione sicura delle chiavi e del relativo ciclo di vita.
- **sicurezza dello sviluppo software e dei sistemi** (11): le Società assicurano lo sviluppo, l'acquisizione, la configurazione, la manutenzione e la dismissione sicuri di sistemi e software secondo principi di security by design, gestione delle vulnerabilità, controllo delle modifiche e verifiche di sicurezza, svolgendo test periodici e valutazione dell'efficacia delle misure adottate e gestendo le relative azioni correttive.
- **change management** (12): le Società assicurano la gestione formalizzata delle modifiche ai sistemi ICT, inclusa valutazione preventiva dell'impatto e del rischio, testing, approvazione, gestione delle modifiche urgenti e verifica post-implementazione.
- **gestione del monitoraggio eventi** (13): le Società assicurano la registrazione, protezione, conservazione e analisi dei log e degli eventi di sicurezza, garantendone integrità, disponibilità per il periodo previsto e sincronizzazione temporale per supportare il rilevamento delle anomalie, la gestione degli incidenti e le attività di audit e investigazione.
- **sicurezza fisica** (14): le Società assicurano la protezione fisica e ambientale delle informazioni, dei sistemi informativi e di rete e delle relative infrastrutture mediante misure proporzionate alla criticità degli asset e ai rischi associati, volte a prevenire accessi non autorizzati, danneggiamenti, furti, interferenze ed eventi ambientali, garantendo la sicurezza delle aree critiche, delle apparecchiature e delle condizioni necessarie alla continuità operativa.
- **gestione della formazione e consapevolezza** (15): le Società assicurano programmi periodici di formazione, addestramento e sensibilizzazione in materia di sicurezza informatica, diffe-

renziati in funzione dei ruoli e delle responsabilità, inclusi gli organi di amministrazione e direttivi. Annotano le attività in un apposito registro aggiornato almeno annualmente.

Le misure sono definite e applicate secondo criteri di adeguatezza e proporzionalità ai sistemi informativi e di rete rilevanti, individuati e mantenuti aggiornati in apposito elenco, nonché agli asset, ai processi e ai servizi da essi supportati.
Le Società assicurano il costante monitoraggio e la misurazione dell'efficacia delle misure di sicurezza attraverso indicatori, verifiche, audit e riesami periodici, con gestione documentata delle non conformità e delle azioni correttive.
Le politiche e i relativi documenti attuativi sono approvati secondo le competenze previste dalla normativa e regolamenti applicabili, comunicati alle articolazioni interessate e riesaminati almeno annualmente, nonché in caso di evoluzioni normative, incidenti significativi, variazioni organizzative, tecnologiche o dell'esposizione alle minacce.
Gli esiti del riesame delle politiche e dei relativi documenti attuativi, gli scostamenti rilevati, le eventuali misure compensative e le conseguenti azioni di adeguamento sono documentati, monitorati e rendicontati agli organi di amministrazione e agli altri organi competenti.



9 ORGANIZZAZIONE DELLA SICUREZZA INFORMATICA

Al fine di assicurare un'efficace gestione dei rischi di sicurezza delle informazioni e di sicurezza cyber, il Gruppo NOVOMATIC adotta un modello organizzativo centralizzato definito in funzione degli obblighi normativi e regolamentari applicabili alle diverse Società e disciplina ruoli, responsabilità, modalità di coordinamento e presidi operativi per la protezione delle informazioni, dei sistemi informativi, delle reti e dei servizi digitali. Il modello assicura il coinvolgimento degli Organi Amministrativi e delle funzioni aziendali competenti, il presidio degli obblighi applicabili, la gestione dei rischi e degli incidenti e il miglioramento continuo delle misure di sicurezza.
Al fine di garantire la chiara attribuzione delle responsabilità e l'efficace governo della sicurezza informatica, il Gruppo predispone specifici documenti organizzativi contenenti ruoli, responsabilità, e organigramma della sicurezza informatica. Tali documenti sono sottoposti a revisione e aggiornamento con cadenza almeno biennale, nonché ogniqualvolta intervengano modifiche organizzative, normative o operative rilevanti.
Il modello centralizzato di Gruppo non modifica le responsabilità attribuite dalla normativa agli organi di amministrazione e direttivi di ciascuna Società qualificata come soggetto NIS2 e DORA.

9.1 Responsabilità degli Organi di Amministrazione

Gli organi di amministrazione approvano le misure di gestione dei rischi per la sicurezza informatica, sovrintendono alla loro attuazione, ricevono periodicamente informazioni sullo stato della sicurezza informatica e sugli incidenti significativi e assicurano lo svolgimento della formazione e degli aggiornamenti previsti dalla normativa applicabile.

10 CICLO DI VITA DELLA POLITICA E RESPONSABILITÀ

La Politica viene rivista secondo quanto previsto al precedente paragrafo 4, ed 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 delle funzioni responsabili del Sistema di Gestione e della funzione Governance & Awareness, dispone dell'autorità e della responsabilità necessarie per attuare e mantenere il controllo sull'applicazione e sull'efficacia del Sistema di Gestione.

POLITICA AZIENDALE DELLA SICUREZZA DELLE INFORMAZIONI - LIFECYCLE



11 ADOZIONE DELLA POLITICA

La presente Politica costituisce il documento di riferimento delle Società del Gruppo in[CC2.1][2.2] materia di sicurezza delle informazioni e sicurezza informatica e definisce principi, indirizzi strategici, responsabilità e criteri organizzativi applicabili nell'ambito descritto al Capitolo 3.
La Politica è adottata formalizzandone il recepimento nel Consiglio di amministrazione di ciascuna Società, come richiesto dalla normativa applicabile, con particolare riferimento agli obblighi previsti dal D.lgs. 138/2024 per i soggetti NIS e dal Regolamento (UE) 2022/2554 per Admiral Pay.

12 MONITORAGGIO E REVISIONE DELLA POLITICA

La presente Politica costituisce il documento di riferimento delle Società del Gruppo in[CC2.1] [2.2] materia di sicurezza delle informazioni e sicurezza informatica e definisce principi, indirizzi strategici, responsabilità e criteri organizzativi applicabili nell'ambito descritto al Capitolo 3.
La Politica è adottata formalizzandone il recepimento nel Consiglio di amministrazione di ciascuna Società, come richiesto dalla normativa applicabile, con particolare riferimento agli obblighi previsti dal D.lgs. 138/2024 per i soggetti NIS e dal Regolamento (UE) 2022/2554 per Admiral Pay.

La Direzione


NOVOMATIC
ITALIA