Politica per la Sicurezza

delle Informazioni e dei Dati

Emissione RSGI	Data	01/07/2024	Firma	*Maria Elisabetta Scipione*
Verifica e Approvazione AU	Data	01/07/2024	Firma	*Maria Fontana*

rev.	Data	Descrizione Aggiornamento	Autore
1	01/07/2024	Prima versione	Maria Elisabetta Scipione

Indice

Sommario

1. Overview della Politica

1.1. Introduzione

Le informazioni sono risorse che, al pari degli altri elementi aziendali, sono essenziali per l'attività di Nike e, di conseguenza, devono essere adeguatamente protette.
Tale aspetto risultadi particolare importanza specialmente per la crescente interconnessione degli ambienti aziendali.
Ilrisultato di questa crescente interconnessione è che le informazioni sono ora esposte ad un crescente numero e una più ampia varietà di minacce e vulnerabilità.
La presente Politica indirizza la gestione della sicurezza delle informazioni all'interno di Nike Web Consulting per assicurare adeguati livelli di sicurezza per le informazioni conservate e trasmesse attraverso tecnologie informatiche tenendo in considerazione i requisiti legali e un'efficace gestione del rischio.

1.2. Obiettivo

Lo scopo del presente documento è quello di fornire una descrizione delle politiche di sicurezza da adottare all'interno del Nike Web Consulting per garantire un adeguato livello di protezione delle informazioni in termini di:

- Riservatezza, assicurando che le informazioni siano accessibili solo agli utenti autorizzati;
- Integrità, salvaguardando completezza, accuratezza e conformità delle informazioni durante le attività di acquisizione, conservazione, elaborazione e condivisione;
- Disponibilità, assicurando che agli utenti autorizzati siano disponibili le informazioni di cui hanno bisogno per svolgere le proprie attività.

Le politiche di sicurezza delle informazioni sono state definite in conformità agli standard internazionali (es. ISO/IEC 27001) e alle norme relative alle pratiche di gestione della sicurezza delle informazioni, agli aspetti di rischio che caratterizzano l'organizzazione e ai relativi requisiti di business.

1.3. Riferimenti

Riferimenti esterni:

- Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni [ISO/IEC 27001]
- Sicurezza delle informazioni, cyber security e protezione della privacy - Controlli di sicurezza delle informazioni [ISO/IEC 27002]
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [Regolamento generale sulla protezione dei dati o GDPR]
- REGOLAMENTO PER LE INFRASTRUTTURE DIGITALI E PER I SERVIZI CLOUD PER LA PUBBLICA AMMINISTRAZIONE (ACN del 27/06/2024)

1.4. Termini e definizioni

Per gli obiettivi di questo documento, di seguito sono riportati termini e definizioni.

Termini	Definizioni
Controllo degliaccessi	Strumenti che permettono di impostare l'accesso fisico e logico agli asset aziendali in modo che sia autorizzato e limitato in base ai requisiti di business e di sicurezza
Asset	Qualsiasi bene che abbia valore per l'organizzazione
Attacco	Tentativo non autorizzato di distruggere, esporre, alterare o qualsiasi tentativo di disattivare, rubare, accedere o fare un uso non autorizzatodi un bene aziendale
Autenticazione	Processo che assicura la verifica dell'identità di un utente o un'entità
Utente autorizzato	Soggetto che possiede una formale autorizzazione ad accedere alle informazioni
Controllo	Misura a presidio di uno specifico rischio
Disaster Recovery	L'insieme delle misure tecnologiche e organizzative progettate per ripristinare sistemi, dati e infrastrutture dopo il verificarsi di un evento che interrompe i processi aziendali
Informazioni	Insieme di dati correlati che hanno valore per l'organizzazione
Evento relativo alla sicurezza delle informazioni	Occorrenza che indica una possibile violazione della sicurezza delle informazioni o un fallimento delle misure adottate

Incidente relativo alla sicurezza delle informazioni	Uno o più eventi di sicurezza delle informazioni correlati e identificati che possono danneggiare le risorse dell'organizzazione o compromettere le sue operazioni

Termini	**Definizioni**
Gestione degli incidenti relativi allasicurezza delle informazioni	Insieme delle attività per la gestione coerente ed efficace degli incidentidi sicurezza delle informazioni
Sistema Informativo	Insieme di applicazioni, servizi, risorse informatiche o altri componenti di gestione delle informazioni
Legal Entity	Organizzazione che possiede diritti e responsabilità legali
Dati Personali	Qualsiasi informazione che (a) può essere usata per stabilire un collegamento tra l'informazione e la persona fisica a cui tale informazione si riferisce, o (b) è o può essere direttamente o indirettamente collegata a una persona fisica
Politica	Intenzioni e direzione di un'organizzazione, come formalmente espressa dal suo top management
Procedura	Modo specifico di svolgere un'attività o un processo
Processo	Insieme di attività interconnesse o interagenti che trasformano gli input in output
Regola	Principio accettato o istruzione che dichiara le aspettative dell'organizzazione su cosa deve essere fatto, cosa è permesso o non permesso
Minaccia	Potenziale causa di un incidente che può provocare danni a un sistema o a un'organizzazione
Utente	Soggetto con accesso ai sistemi informativi dell'organizzazione

2. Politiche per la sicurezza delle informazioni

Nike Web Consulting ha definito i domini di sicurezza da presidiare con apposite procedure di sicurezza informatica.
I domini di sicurezza delle informazioni sono suddivisi in quattro aree (Controlli organizzativi, Controlli sul personale, Controlli fisici e Controlli tecnologici) e sono descritti nei paragrafi seguenti.

- Controlli organizzativi
  - Ruoli e Responsabilità nella sicurezza delle informazioni
  - Gestione degli asset
  - Classificazione delle informazioni
  - Controllo degli accessi
  - Sicurezza delle informazioni nelle terze parti
  - Compliance

- Controlli sul personale
  - Sicurezza delle Risorse Umane

- Controlli fisici
  - Sicurezza fisica
  - Sicurezza ambientale

- Controlli tecnologici
  - Sicurezza delle operazioni
  - Sicurezza delle comunicazioni
  - Ciclo di vita sicuro del sistema e del software
  - Gestione della Business Continuity e Disaster Recovery

2.1. Controlli organizzativi

2.1.1. Ruoli e Responsabilità nella sicurezza delle informazioni

A livello aziendale, i ruoli e le responsabilità riguardanti la sicurezza delle informazioni e la gestione dei rischi correlati sono i seguenti.

- Responsabile Sistemi IT (RSI)
  - Gestisce il rischio di sicurezza delle informazioni durante l'intero ciclo di vita dei dati, assicurando l'esecuzione di valutazioni periodiche del rischio per identificare le priorità per la gestione dei rischi di sicurezza delle informazioni e per l'attuazione di controlli per ridurre tali rischi;
  - Informa sullo stato e sui rischi di cyber security, assumendo anche il ruolo di referente per la strategia globale e il budget necessario;
  - Gestisce/sovrintende il team che si occupa delle tematiche relative alla sicurezza delle informazioni;

- Mantiene aggiornate le procedure di sicurezza delle informazioni di Gruppo;
- Assicura, attraverso valutazioni periodiche, l'efficacia delle misure di sicurezza delle informazioni al fine di proteggere il patrimonio aziendale e garantire il rispetto delle norme relative alle pratiche di gestione della sicurezza delle informazioni e dei requisiti aziendali;
- Esegue attività di controllo della sicurezza delle informazioni sulla catena di fornitura e su altre terze parti rilevanti;
- Supporta le attività di controllo della sicurezza delle informazioni richieste da terze parti;
- Gestisce la progettazione di soluzioni appropriate per la sicurezza delle informazioni;
- Gestisce le attività di rilevamento e risposta agli incidenti di sicurezza delle informazioni.

- Gruppo IT
  - Allinea le tecnologie dell'informazione alla strategia di sicurezza dell'informazione delGruppo;
  - Implementa le soluzioni di sicurezza delle informazioni progettate dal Group IT Security Manager;
  - Fornisce supporto nella attività di valutazione periodica in ambito sicurezza delle informazioni;
  - Implementa le iniziative di rimedio identificate a valle delle attività di valutazione periodica in ambito sicurezza delle informazioni;
  - Fornisce supporto nelle attività di rilevamento e risposta agli incidenti di sicurezza delleinformazioni;
  - Gestisce le attività di recupero degli incidenti di sicurezza delle informazioni;
  - Esegue le attività tecniche per mantenere aggiornate le risorse tecniche IT.

2.1.2. Gestione degli asset

Tutti gli asset tecnologici (hardware, software e risorse di rete) associati alle informazioni devono essere identificati e registrati in un inventario mantenuto aggiornato (**Mod-710-M-Inventario degli asset)**.

Le regole per l'uso accettabile degli asset devono essere identificate e documentate al fine di garantirne il corretto e sicuro funzionamento e per ridurre e prevenire i rischi (inclusi attacchi di virus, compromissione di sistemi e servizi di rete, questioni legali) legati ad un uso inappropriato (ad esempio, errori umani, furti, frodi o usi impropri).

I dipendenti e gli utenti esterni che utilizzano o hanno accesso agli asset di Nike Web Consulting devono essere resi consapevoli dei requisiti di sicurezza definiti o e devono essere resi responsabili di ogni utilizzo delle risorse informatiche aziendali.

Tutti i dipendenti e gli utenti esterni devono restituire tutti i beni aziendali loro concessi al termine

del rapporto di lavoro, del contratto o dell'accordo di collaborazione.

2.1.3. Classificazione delle informazioni

Le informazioni del Nike Web Consulting devono essere classificate ed etichettate in termini di valore, sensibilità e criticità aziendale e in base ai requisiti legali. Oltre ai dati di tipo ordinario, devono essere valutati i dati sensibili e critici (di volta in volta in base ai dati trattati durante l'erogazione del servizio).
Tutti i dati devono avere un indice di classificazione come da **PROC-750 Informazioni Documentate.**
I proprietari dei dati sono responsabili dell'identificazione di eventuali requisiti aggiuntivi per dati specifici o eccezioni ai requisiti di gestione standard.
I sistemi e le applicazioni informatiche devono essere classificati in base alla classificazione più elevata dei dati che memorizzano o elaborano.

2.1.4. Controllo degli accessi

Il controllo degli accessi è regolato da procedura di sicurezza **PSI-01 Controllo dell'accesso**.

2.1.5. Sicurezza delle informazioni nelle terze parti

In caso di accesso di terze parti alle informazioni, sono stabilite adeguate misure di sicurezza per garantire la riservatezza, l'integrità e la disponibilità delle informazioni.

Gli accordi con le terze parti includono requisiti relativi alla protezione dei dati del Nike Web Consulting. In particolare, le terze parti saranno disponibili a condividere, su richiesta, i loro piani di sicurezza e le misure di sicurezza implementate e consentire verifiche di sicurezza da partedel Nike Web Consulting.
I Service Level Agreement (SLA) devono essere inclusi nei contratti con le terze parti per definire puntualmente i livelli di servizio. I servizi forniti dalle terze parti devono essere monitorati periodicamente.

2.1.6. Compliance

La gestione dei sistemi informativi adottati nel Nike Web Consulting deve essere conforme alle leggi (es. GDPR), agli standard e alle politiche aziendali per prevenire i rischi di non conformità e le relative conseguenze (es. sanzioni, danni di reputazione, penali contrattuali, ecc.).

2.2. Controlli sul personale

2.2.1. Sicurezza delle Risorse Umane

Durante il processo di assunzione di personale, le attività di verifica effettuate dal Responsabile del Personale sui candidati devono essere proporzionate ai requisiti aziendali, alla classificazione delle informazioni a cui tali candidati potranno/dovranno accedere e ai relativi rischi associati.
Gli accordi contrattuali con i dipendenti e i collaboratori devono specificare le loro responsabilità in tema di sicurezza delle informazioni.
I dipendenti e i collaboratori devono essere consapevoli delle minacce e istruiti sul corretto utilizzo dei sistemi informativi e dei dispositivi di proprietà del Nike Web Consulting (attività di sensibilizzazione e formazione).
I dipendenti e i collaboratori devono essere consapevoli che le loro responsabilità e i loro doveri in materia di sicurezza delle informazioni rimangono validi anche dopo la cessazione o la modifica del rapporto di lavoro o di collaborazione. I diritti di accesso attribuiti ai dipendenti e collaboratori in relazione alle informazioni e alle strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapportodi lavoro o di collaborazione o aggiornati in seguito a cambiamenti intercorsi.

2.3. Controlli fisici

2.3.1. Sicurezza fisica

Le misure di controllo inerenti gli accessi fisici sono definite nella **PSI-02 Sicurezza fisica.**

2.3.2. Sicurezza ambientale

Le misure di controllo di sicurezza ambientale sono definite nella PSI-02 Sicurezza fisica.
Gli ambienti di lavoro devono rispettare le politiche di Gruppo in materia di salute e sicurezza.

2.4. Controlli tecnologici

2.4.1. Sicurezza delle operazioni

Le modifiche all'organizzazione, ai processi aziendali, alle strutture di elaborazione delle informazioni e ai sistemi che influiscono sulla sicurezza delle informazioni devono essere controllate e documentate (Change Management).
L'uso delle risorse è monitorato e sono effettuate proiezioni sui requisiti futuri in termini di capacità per garantire il mantenimento del livello delle prestazioni dei servizi IT (Capacity Management), tenendo conto della criticità del business dei sistemi interessati.
Il back-up delle informazioni del Nike Web Consulting è effettuato e testato regolarmente per mantenere la disponibilità dei dati in linea con i rischi associati. Inoltre, il software e le strutture di elaborazione delle informazioni sono protetti da codici malevoli per garantire l'integrità delsoftware e delle informazioni.
I log degli eventi che tengono traccia delle attività degli utenti, degli amministratori e degli operatori di sistema, delle eccezioni, dei guasti e degli eventi relativi alla sicurezza delle informazioni, devono essere prodotti, conservati e rivisti regolarmente. Le attività di registrazione devono essere eseguite in conformità alla legislazione vigente.
Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere oggetto di valutazione e devono essere adottate misure appropriate per affrontare il rischio associato.

2.4.2. Sicurezza delle comunicazioni

I dispositivi di comunicazione e di rete devono essere protetti per garantire l'integrità, la riservatezza e la disponibilità dei dati. La sicurezza dei dispositivi di rete deve essere configurata correttamente, per assicurare la corretta segregazione tra i diversi ambienti di utilizzo. La sicurezza relativa allo scambio di dati tra luoghi fisici distinti e con le terze parti deve essere affrontata anche per mezzo di specifiche misure di sicurezza (ad esempio implementando la crittografia dei dati).

2.4.3. Ciclo di vita sicuro del sistema e del software

Il ciclo di vita di sviluppo del sistema e le sue fasi (installazione, configurazione, manutenzione e dismissione) devono essere chiaramente definiti per prevenire la perdita di dati o la modifica non autorizzata. Gli ambienti di sviluppo, test e produzione devono essere segregati e l'accesso al codice

sorgente del programma deve essere limitato.
Devono essere definite politiche per valutare le misure di sicurezza relative all'adozione di servizi Cloud e dispositivi di Mobile Computing.

2.4.4. Gestione degli incidenti relativi alla sicurezza delle informazioni

Gli eventi di sicurezza e le vulnerabilità associate ai sistemi informativi devono essere comunicate tempestivamente per intraprendere le appropriate azioni correttive.
Devono essere messe in atto procedure di segnalazione e di escalation degli eventi.
Tutti i dipendenti e i collaboratori devono essere informati su come poter segnalare le diverse tipologie di eventi che potrebbero avere un impatto sulla sicurezza degli asset informatici del Nike Web Consulting.

Le attività di gestione degli incidenti di sicurezza delle informazioni devono essere allineate al processo definito a livello di Gruppo. In caso di violazione di dati personali, le attività di gestione devono essere conformi ai requisiti normativi vigenti (es. GDPR).

2.4.5. Gestione della Business Continuity e Disaster Recovery

Un sistema di gestione della Business Continuity è un insieme di processi, procedure e sistemi tecnologici finalizzati a garantire la continuità delle attività aziendali, in caso di eventi/disastri significativi, minimizzando i relativi impatti.
Per definire un sistema di gestione della Business Continuity è stato analizzato il contesto di business del Nike Web Consulting, definite le relative strategie di continuità operativa e le misure tecnologiche ed organizzative per ripristinare sistemi, dati ed infrastrutture dopo il verificarsi di un evento che interrompa i processi aziendali (Piano di Disaster Recovery).
Il piano di Business Continuity e il piano di Disaster Recovery sono regolarmente testati al fine di verificarne l'efficacia e l'efficienza e rivisti e aggiornati periodicamente in caso di cambiamenti del contesto.
IO-03 rev.6 Piano di Continuità Operativa e Disaster Recovery.

3. Eccezioni

La Direzione può decidere di adottare requisiti più restrittivi rispetto quelli delineati dalla presente Politica. Tali situazioni non sono considerate eccezioni alla Politica e pertanto devono solo essere notificate al RSGI. Le eccezioni a questa Politica devono essere formalmente approvate in conformità ai principi guida di Nike Web Consulting.