POLICY DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

NOVA GROUP SRL
Sede legale: Via Dante,7 Frattamaggiore(NA) 80027
p.iva:11173370963

1. Campo d'applicazione, scopo e destinatari

Lo scopo di questo documento è definire delle chiare regole per l'uso del sistema informativo e di altre risorse informative all'interno di NOVA GROUP S.R.L.

Destinatari di questo documento sono tutti dipendenti/collaboratori/fornitori di NOVA GROUP S.R.L.

2. Regole di Sicurezza di Base

2.1. Definizioni

Sistema informativo: include tutti i server e i client, l'infrastruttura di rete, il software di sistema e applicativo, i dati e altri sottosistemi e componenti di computer che sono di proprietà o utilizzati dall'organizzazione o che sono sotto la responsabilità dell'organizzazione. L'uso di un sistema informativo include anche l'uso di tutti i servizi interni o esterni, come l'accesso a Internet, l'e-mail, ecc.

Risorse informative: nel contesto di questa politica, il termine risorsa informativa viene applicato ai sistemi di informazione e ad altre informazioni / attrezzature inclusi documenti cartacei, telefoni cellulari, computer portatili, supporti di memorizzazione di dati, ecc.

2.2. Utilizzo accettabile

Le risorse informative possono essere utilizzate solo per esigenze aziendali allo scopo di eseguire attività correlate all'organizzazione.

2.3. Responsabilità per le risorse

Ogni risorsa informativa ha un proprietario designato nell'Elenco delle attività. Il proprietario della risorsa è responsabile per la riservatezza, l'integrità e la disponibilità delle informazioni nella risorsa in questione.

2.4. Attività vietate

È vietato utilizzare le risorse informative in modo da occupare inutilmente capacità, indebolire le prestazioni del sistema informativo o rappresentare una minaccia alla sicurezza. È inoltre vietato:

- scaricare file di immagini o video che non hanno uno scopo commerciale, inviare catene di e-mail, giocare, ecc.
- installare software su un computer locale senza autorizzazione esplicita da parte dell'Amministratore IT
- utilizzare applicazioni Java, controlli Active X e altri codici mobili, tranne se autorizzato dall'Amministratore IT
- utilizzare strumenti crittografici (cifratura) su un computer locale, tranne nei casi specificati nella Politica di Classificazione delle Informazioni
- scaricare il codice del programma da un supporto esterno
- installare o utilizzare dispositivi periferici quali modem, schede di memoria o altri dispositivi per la memorizzazione e la lettura di dati (ad esempio unità flash USB) senza autorizzazione esplicita da parte dell'Amministratore IT; l'uso in conformità con la Politica di Classificazione delle Informazioni è consentito.

2.5. Portare delle risorse fuori dal sito

Apparecchiature, informazioni o software, indipendentemente dalla forma o supporto di memorizzazione, non possono essere portati fuori dai locali aziendali senza autorizzazione scritta (dalla durata massima pari alla giornata lavorativa) da parte dell'Amministratore IT.

Finché tali beni sono al di fuori dell'organizzazione, devono essere controllati dalla persona a cui è stata concessa l'autorizzazione per la loro rimozione.

2.6. Restituzione di beni in caso di risoluzione del contratto

Alla conclusione di un contratto di impiego o di un altro contratto in base al quale vengono utilizzate varie apparecchiature, software o informazioni in formato elettronico o cartaceo, l'utente deve restituire tutte tali risorse informative all'Amministratore IT.

2.7. Procedure di backup

Le eventuali procedure di backup sono in capo e possono essere realizzate esclusivamente dell'Amministratore IT.

I backup possono interessare la parte web, database, e file di configurazioni dei sistemi server.

I dati dei PC utente non subiscono una procedura di back-up, e ciò in quanto gli utenti non possono utilizzare dati in locale.

Viene, inoltre, utilizzato un CRM-CLOUD SIDIAL sul quale vengono salvati i dati.

2.8. Protezione antivirus

Il sistema antivirus deve essere installato su ogni computer e/o ogni postazione anche mobile, con attivazione di aggiornamenti automatici, e ciò preferibilmente con sistema a pagamento che possa garantire adeguati livelli di sicurezza.

2.9. Autorizzazioni per l'uso del sistema informativo

Gli utenti del sistema informativo possono accedere solo a quelle risorse del sistema informativo per le quali sono state esplicitamente autorizzati dal titolare della risorsa.

Gli utenti possono utilizzare il sistema informativo solo per gli scopi per i quali sono stati autorizzati, ovvero per i quali hanno ottenuto i diritti di accesso.

Gli utenti non devono prendere parte ad attività che possono essere utilizzate per aggirare i controlli di sicurezza del sistema di informazione.

2.10. Responsabilità dell'account utente

L'utente non deve, direttamente o indirettamente, consentire a un'altra persona di utilizzare i suoi diritti di accesso, cioè il nome utente, e non deve utilizzare il nome utente e / o la password di un'altra persona. L'uso di nomi utente di gruppo è vietato.

Il proprietario dell'account utente è il suo utente, che è responsabile del suo utilizzo e di tutte le transazioni eseguite attraverso questo account utente.

2.11. Responsabilità relative alla password

Gli utenti devono applicare buone pratiche di sicurezza quando selezionano e usano le password:

- le password non devono essere divulgate ad altre persone, inclusi gli amministratori di gestione e di sistema
- le password non devono essere trascritte, a meno che un metodo sicuro sia stato approvato dall'Amministratore IT
- le password generate dall'utente non devono essere distribuite attraverso alcun canale (utilizzando la distribuzione orale, scritta o elettronica, ecc.)
- le password devono essere cambiate se vi sono indicazioni che le password o il sistema potrebbero essere stati compromessi - in tal caso deve essere segnalato un incidente di sicurezza
- È necessario selezionare password complesse, nel modo seguente:
  - o utilizzando almeno otto-dieci caratteri

o utilizzando almeno un carattere numerico

o utilizzando almeno un carattere alfabetico maiuscolo e almeno uno minuscolo

o una password non deve essere una parola del dizionario, una parola dialettale o gergale di qualsiasi lingua, o una qualsiasi di queste parole scritte al contrario

o le password non devono essere basate su dati personali (ad esempio data di nascita, indirizzo, nome di un familiare, ecc.)

o le ultime tre password non devono essere riutilizzate

- le password scadono e devono essere aggiornate ogni 4 mesi (sul Dominio Utente)
- la password deve essere cambiata al primo accesso a un sistema
- le password non devono essere memorizzate in un sistema di accesso automatico (ad esempio macro o browser)
- le password utilizzate per scopi privati non devono essere utilizzate per scopi commerciali

2.12. Navigazione web

È possibile accedere a Internet solo attraverso la rete locale dell'organizzazione con un'infrastruttura adeguata e una protezione firewall. È vietato l'accesso diretto a Internet tramite modem, Internet mobile o altri dispositivi per l'accesso diretto a Internet.

È consentito accedere alla rete wireless esclusivamente al personale autorizzato.

L'Amministratore IT può bloccare l'accesso ad alcune pagine Internet per singoli utenti, gruppi di utenti o tutti i dipendenti dell'organizzazione, con creazione di specifica white list. Se l'accesso ad alcune pagine Web è bloccato, l'utente può inviare una richiesta scritta all'Amministratore IT per ottenere l'autorizzazione ad accedere a tali pagine. L'utente non deve cercare di aggirare tale restrizione autonomamente.

L'utente deve considerare le informazioni ricevute attraverso siti Web non verificati come inaffidabili.

L'utente è responsabile di tutte le possibili conseguenze derivanti dall'uso non autorizzato o inappropriato di servizi o contenuti Internet, con valutazione di ordine disciplinare, anche ai sensi e per gli effetti dell'art. 7, L. 300/70 ì, nonché della sezione disciplinare del CCNL applicato.

2.13. E-mail e altri metodi di scambio di messaggi

I metodi di scambio di informazioni sulle attività aziendali comprendono esclusivamente l'utilizzo della Posta Elettronica, comprendente le restrizioni su chi è autorizzato a utilizzare canali di comunicazione, ossia definisce quali attività siano vietate.

Gli utenti possono solo inviare messaggi contenenti informazioni veritiere. È vietato inviare materiali con contenuti inquietanti, spiacevoli, sessualmente espliciti, scortesi, diffamatori o altri contenuti inaccettabili o illegali. Gli utenti non devono inviare messaggi di spam a persone con le quali non è stato stabilito alcun rapporto commerciale o a persone che non hanno richiesto tali informazioni.

Se un utente riceve un'e-mail di spam, deve informare l'Amministratore IT.

Se si invia un messaggio con un'etichetta di riservatezza, l'utente deve proteggerlo come specificato nella Politica di Classificazione delle Informazioni.

L'utente deve salvare ogni messaggio contenente dati significativi per l'attività dell'organizzazione utilizzando il metodo specificato dall'Amministratore IT.

Ogni messaggio di posta elettronica deve contenere una dichiarazione di non responsabilità, ad eccezione dei messaggi inviati tramite i sistemi di comunicazione determinati dall'Amministratore IT. Se un utente pubblica un messaggio su un sistema di scambio di messaggi (social network, forum, ecc.), deve dichiarare in modo inequivocabile che non esprime il punto di vista dell'organizzazione.

Per quanto non espressamente indicato si rinvia alla policy di cui al Codice Etico.

2.14. Copyright

Gli utenti non devono fare copie non autorizzate di software di proprietà dell'organizzazione, tranne nei casi consentiti dalla legge, dal proprietario o Amministratore IT.

Gli utenti non devono copiare software o altri materiali originali da altre fonti e sono responsabili per tutte le conseguenze che potrebbero derivare dalla legge sulla proprietà intellettuale.

Il responsabile per questo documento è il DPO, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.