POLICY AZIENDALI

Le policy aziendali comprendono diverse politiche che trattano diversi temi:

- **Politica di sicurezza informatica**: Questa politica stabilisce le procedure di sicurezza che i dipendenti devono seguire per garantire che i dati aziendali siano protetti da accessi non autorizzati, furti o perdite di dati. La politica di sicurezza informatica può includere l'uso di password sicure, l'autenticazione a due fattori, la crittografia dei dati, la verifica delle vulnerabilità e l'aggiornamento costante del software antivirus.
- **Politica di uso accettabile**: Questa politica definisce l'uso consentito e non consentito dei sistemi informativi aziendali da parte dei dipendenti. Ciò include la definizione delle attività che sono permesse e quelle che sono proibite, come l'accesso a siti web non pertinenti al lavoro o l'uso di software piratato.
- **Politica di accesso remoto**: Questa politica definisce le regole e le procedure per l'accesso remoto ai sistemi informativi aziendali da parte dei dipendenti. Ciò include l'utilizzo di una VPN sicura, l'accesso tramite dispositivi autorizzati e l'implementazione di controlli di sicurezza per garantire che solo le persone autorizzate possano accedere ai dati.
- **Politica di gestione dei dispositivi mobili**: Questa politica stabilisce le regole per l'uso dei dispositivi mobili aziendali, come smartphone e tablet. Ciò include la sicurezza dei dati, l'utilizzo di password, la crittografia dei dati, la disattivazione remota e la pulizia dei dati in caso di smarrimento o furto.
- **Politica di backup dei dati**: Questa politica definisce le procedure per il backup dei dati aziendali. Ciò include la pianificazione dei backup regolari, la conservazione sicura dei backup e il test periodico della capacità di ripristino dei dati.
- **Politica di gestione delle password**: Questa politica definisce le regole per la creazione, la gestione e la protezione delle password aziendali. Ciò include l'uso di password complesse, la rotazione regolare delle password e la protezione delle password da accessi non autorizzati.
- **Politica di formazione sulla sicurezza informatica**: Questa politica prevede la formazione regolare dei dipendenti sulle procedure di sicurezza informatica e sulle minacce alla sicurezza dei dati. Ciò include l'identificazione dei tentativi di phishing, la prevenzione degli attacchi ransomware e l'uso sicuro delle reti WiFi pubbliche.
- **Politica di reportistica delle violazioni della sicurezza**: Questa politica definisce le procedure per la segnalazione delle violazioni della sicurezza informatica da parte dei dipendenti. Ciò include l'obbligo di segnalare qualsiasi incidente o tentativo di accesso non autorizzato ai dati aziendali, così che la società possa rispondere tempestivamente e prendere le misure necessarie per proteggere i dati.

Esempi di policy:

- consorziodibonificachiese
- cgil
- illimity
- aterpadova

Policy gestione delle password

Scopo

Questa policy definisce le norme per la creazione, la gestione e l'utilizzo delle password per l'accesso ai sistemi e alle risorse dell'azienda, al fine di proteggere le informazioni aziendali e di prevenire accessi non autorizzati.

Ambito Di Applicazione

Questa policy si applica a tutti i dipendenti, collaboratori, consulenti e terze parti che utilizzano i sistemi e le risorse dell'azienda.

Terminologia

Password: Sequenza di caratteri utilizzata per l'accesso ai sistemi e alle risorse dell'azienda.

Account: Credenziali di accesso di un utente, che includono un nome utente e una password.

Password temporanea: Password generata dal sistema o assegnata dall'amministratore, che deve essere cambiata al primo accesso.

Blocco dell'account: Sospensione temporanea dell'account a causa di accessi non autorizzati o di password errate inserite troppo volte.

Policy

- **Complessità delle password**
  - Le password devono essere complesse e difficili da indovinare. Devono includere una combinazione di lettere (minuscole e maiuscole), numeri, simboli e caratteri speciali. La lunghezza minima delle password deve essere di 8 caratteri. Le password devono essere cambiate almeno ogni 90 giorni.
- **Limitazione dell'uso della stessa password**
  - Gli utenti non devono utilizzare la stessa password per più di un account. Inoltre, gli utenti non devono utilizzare la stessa password per un periodo di tempo prolungato. Le password temporanee devono essere cambiate immediatamente al primo accesso.
- **Memorizzazione delle password**
  - Le password non devono essere scritte su carta o inviate via e-mail. Inoltre, le password non devono essere salvate in chiaro sul computer o in qualsiasi altro dispositivo di archiviazione. Si consiglia di utilizzare un software di gestione delle password affidabile.
- **Accesso ai dati sensibili**
  - Gli utenti devono utilizzare password univoche per accedere a dati sensibili o critici. Inoltre, gli utenti devono avere accesso solo ai dati necessari per svolgere le loro attività lavorative.
- **Blocco dell'account**
  - Se un utente inserisce la password in modo errato per un numero di volte specificato, l'account deve essere bloccato per un periodo di tempo specificato. L'utente deve contattare l'amministratore del sistema per sbloccare l'account.
- **Controllo di accesso**
  - Le password non devono essere condivise tra gli utenti e devono essere utilizzate solo da coloro che hanno il diritto di accedere a determinati dati o sistemi.
- **Formazione degli utenti**
  - Tutti gli utenti dell'organizzazione devono essere informati della policy di gestione delle password e delle conseguenze della non conformità. L'azienda deve fornire formazione e supporto adeguati per garantire che gli utenti comprendano e rispettino la policy.

Conclusione

La gestione delle password è un aspetto importante della sicurezza informatica e richiede la massima attenzione

Policy per la gestione dei backup

Scopo

Questa policy definisce le norme per la creazione, la gestione e la conservazione dei backup dei dati dell'azienda, al fine di garantire la continuità del business, la protezione dei dati e la ripristinabilità dei sistemi in caso di perdita di dati.

Ambito Di Applicazione

Questa policy si applica a tutti i dipendenti, collaboratori, consulenti e terze parti che gestiscono i backup dei dati dell'azienda.

Terminologia

Backup: Copia di dati e informazioni archiviati in un sistema di archiviazione esterno o remoto, creata per la protezione dei dati in caso di perdita o danneggiamento dei dati originali.

Data retention: La durata durante la quale i backup dei dati vengono conservati.

Full backup: Backup completo di tutti i dati presenti su un sistema.

Incremental backup: Backup parziale che include solo i dati modificati dopo l'ultimo backup completo.

Restore: Processo di ripristino dei dati dai backup.

Policy

- **Creazione e conservazione dei backup**
    - Deve essere creato un backup completo di tutti i dati e delle informazioni critici dell'azienda almeno una volta alla settimana. Inoltre, i backup incrementali devono essere creati almeno una volta al giorno. I backup devono essere conservati in un sistema di archiviazione esterno sicuro e in un'ubicazione geograficamente separata dalla sede principale dell'azienda. La durata della conservazione dei backup dei dati deve essere stabilita dal responsabile IT.
- **Verifica dei backup**
    - Deve essere eseguita regolarmente una verifica dei backup per garantire che i dati siano stati copiati correttamente e siano ripristinabili. Questa verifica deve essere eseguita almeno una volta al trimestre.
- **Gestione dei backup**
    - Deve essere designato un responsabile IT per la gestione dei backup dei dati dell'azienda. Questo responsabile deve garantire che i backup vengano creati, verificati e conservati correttamente. Inoltre, il responsabile deve essere responsabile per l'accesso e la sicurezza dei backup dei dati.
- **Protezione dei backup**
    - I backup dei dati devono essere protetti con password e crittografia per prevenire l'accesso non autorizzato. Inoltre, devono essere utilizzati metodi di sicurezza fisica per proteggere i

supporti di backup, come il controllo degli accessi alle aree di archiviazione dei backup e la custodia dei supporti in casse di sicurezza.

- **Formazione degli utenti**
    - Tutti gli utenti dell'organizzazione devono essere informati della policy di backup e delle conseguenze della non conformità. L'azienda deve fornire formazione e supporto adeguati per garantire che gli utenti comprendano e rispettino la policy.

Conclusione

La gestione dei backup dei dati è un aspetto importante della sicurezza informatica e richiede la massima attenzione. La perdita di dati può avere gravi conseguenze per l'attività dell'azienda e la protezione dei dati è essenziale per garantire la continuità del business e la ripristinabilità dei sistemi.