POLITICA ACCESS CONTROL

SCOPO

Questa politica definisce gli utenti che hanno l'accesso e il controllo su dati sensibili o specialmente regolamentati ed è stata progettata per ridurre al minimo il rischio di danni nei confronti delle risorse e dei dati dell'organizzazione. Viene stabilito il privilegio di accesso degli utenti in relazione a dati e dispositivi per permettere agli utenti di eseguire le loro funzioni lavorative senza particolare disagio.

CAMPO DI APPLICAZIONE

Questa politica si applica a tutto il personale dell'organizzazione.

MODALITÀ OPERATIVE

Privilegi del Computer Locale
Ci sono tre categorie principali di utenti su un computer o una rete. Queste categorie includono:

1. Utente Limitato → Può utilizzare il computer e salvare i documenti, ma non può modificare le impostazioni di sistema.
2. Utente Standard → Può modificare le impostazioni di sistema e installare programmi che non coinvolgono i file del sistema operativo.
3. Amministratori → Hanno accesso completo nel leggere e scrivere i dati sul sistema, aggiungere/rimuovere programmi o modificare le impostazioni di sistema.

   La maggior parte degli utenti sulle reti comuni devono essere classificati come "Utente Limitato".
   Solo agli utenti con formazione speciale o necessità di un accesso ulteriore deve essere consentito di cambiare le impostazioni di sistema e installare i programmi che non sono programmi del sistema operativo. Questo perché molti virus, adware (Software sovvenzionato da pubblicità) o spyware (Software spia) possono essere installati in modo da ingannare l'utente. Se l'utente non ha la possibilità di installare programmi o modificare le impostazioni rendendole più vulnerabili, la maggior parte di questi potenziali problemi di sicurezza possono essere evitati.

Il livello di accesso è strettamente legato al ruolo dell'utente, può essere modificato solo dopo la dimostrazione dell'assoluta necessità per lo svolgimento delle funzioni lavorative, inoltre deve essere approvato dal responsabile della sicurezza delle informazioni prima di poter diventare effettivo.

Gruppi che possono essere ammessi ad un tipo di accesso ulteriore includono:
- ⇒ gli Amministratori di Dominio
- ⇒ gli Sviluppatori di applicazioni a scopo di test che hanno una conosciuta educazione o abilità informatica.

Privilegi di Rete
La Maggior parte degli utenti della rete potranno accedere ai seguenti tipi di risorse di rete:

a) E-Mail → la Maggior parte degli utenti avrà pieno accesso alla propria e-mail. Essi non saranno in grado di trasferire la proprietà a qualcun altro.
b) Un personale spazio di archiviazione (drive) su un file server di rete → Si tratta di una cartella in uno spazio di archiviazione che solo l'utente principale di questa unità è in grado di leggere e modificare, con l'eccezione degli

amministratori del dominio. L'utente non potrà trasferire la proprietà a qualcun altro.

c) Un gruppo condiviso della drive → Questa è una cartella a cui i membri di determinati gruppi o divisioni dell'organizzazione possono accedere. L'accesso può essere limitato alla lettura e/o alla scrittura e può variare per esigenze organizzative.

d) Accesso alle banche dati (database) → Ci possono essere ulteriori banche dati che possono essere memorizzate su una drive condivisa, o su qualche altra risorsa. La maggior parte dei database dispone di un livello d'uso standard che consente agli utenti, con un'autorizzazione appropriata, di inserire dati e leggere le informazioni dei report. Tuttavia solo gli amministratori della banca dati avranno pieno accesso a tutte le risorse del database che amministrano.

Gruppi a cui può essere concesso un livello di accesso ulteriore includono:

- Operatore Backup → Ha il permesso di leggere i dati sul dominio con lo scopo di salvare i file sul supporto di backup. Questo gruppo non può modificare i dati di un dominio.
- Operatore Account → E' in grado di gestire e visualizzare le informazioni sull'account utente del dominio.
- Operatore Server → Ha dei privilegi concernenti i server, tra cui la lettura e la scrittura dei dati, l'installazione di programmi, e la modifica delle impostazioni.
- Amministratore Dominio → Ha privilegi su tutti i computer del dominio, compresi i server e workstation. Privilegi includono la lettura e la scrittura dei dati, l'installazione di programmi, e la modifica delle impostazioni.

REGOLAMENTO

Poiché la sicurezza e l'integrità dei dati, insieme alla protezione delle risorse, sono fondamentali per il funzionamento dell'organizzazione, i dipendenti che non rispettano questo regolamento possono essere soggetti a provvedimenti disciplinari, incluso il licenziamento.