ARBONIA

IT SECURITY

Information Security Policy

Politica sulle password

Versione:	1.0
Approvato:	08.07.2021
Stato:	RELEASED
Classificazione:	RESTRICTED
Creato da:	ICT Security Officer
Approvato da:	Arbonia IT Board
Politica:	IS-ISP-GROUP-001-PASSWORD-POLICY_IT
Revisione:	non disponibile

Informazioni sulla politica

Finalità	La politica sulle password descrive e definisce i principi per la creazione, la gestione e l'uso delle password nel gruppo Arbonia.
Utente / destinatario	▪ Tutti i collaboratori del gruppo Arbonia ▪ Appaltatori esterni / fornitori di servizi / clienti e partner che hanno accesso ai sistemi ICT del gruppo Arbonia
Archiviazione elettronica dei documenti	https:\\security.arbonia.com

Prova della modifica

Versione	Data	Stato	Modifica	da parte di
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Indice

Elenco delle abbreviazioni

Termine	Descrizione
ICT	Informations and Communications Technology (tecnologia dell'informazione e della comunicazione)
OS	Operating System (sistema operativo)
ISMS	Sistema di gestione della sicurezza delle informazioni

Glossario

Termine	Descrizione
Attacco brute force (di forza bruta)	Un attacco brute force è un tentativo di decifrare una password o un nome utente provando tutte le possibilità.
Sistema di gestione della sicurezza delle informazioni	Un sistema di gestione della sicurezza delle informazioni è l'istituzione di procedure e regole all'interno di un'organizzazione che servono a definire, gestire, controllare, mantenere e migliorare continuamente la sicurezza delle informazioni in modo permanente.

1 Scopo, ambito e utenti

La politica descrive i requisiti e le specifiche delle password per l'accesso ai sistemi ICT del gruppo Arbonia. Stabilisce le regole per la gestione, l'uso e la creazione sicura delle password.

La politica si applica all'intero ambito del sistema di gestione della sicurezza delle informazioni (ISMS), cioè a tutti i sistemi ICT del gruppo Arbonia.

Gli utenti e i destinatari di questa politica sono tutti i collaboratori del gruppo Arbonia così come gli appaltatori esterni / fornitori di servizi / clienti / partner ecc. che necessitano dell'accesso ai sistemi ICT del gruppo Arbonia.

2 Principi di governance

2.1 Importanza delle password

La sicurezza dei sistemi ICT di Arbonia si basa, tra l'altro, sulla cura con cui vengono gestite le password e, soprattutto, sul rispetto dei principi di base dell'uso delle password.

Uno dei principali obiettivi degli aggressori è quello di rubare le credenziali di un utente al fine di ottenere l'accesso ai sistemi ICT del gruppo Arbonia e quindi trovare e sfruttare eventuali vulnerabilità. Questi cercano di acquisire autorizzazioni privilegiate di un amministratore di sistema, con le quali possono, nel peggiore dei casi, realizzare varie attività come il furto di dati, lo spionaggio o l'installazione di malware senza essere notati. Per questo motivo, le password deboli, così come la loro gestione impropria, rappresentano un rischio significativo. Questo rischio viene ulteriormente aumentato con l'uso necessario di credenziali privilegiate, che sono spesso necessarie per eseguire attività lavorative.

È quindi imperativo prevenire il furto dei dati di accesso e osservare i seguenti obblighi.

2.2 Obblighi degli utenti / dei titolari di account

Tutti gli utenti devono applicare procedure comprovate e sicure durante la selezione e l'utilizzo delle password (ulteriori dettagli al capitolo 3):

- È sempre necessario scegliere una password «forte». La lunghezza e il formato di una password devono essere scelti in modo che un attacco brute force richieda tempo e non porti al successo
- Le password non devono essere rivelate ad altre persone. Nemmeno a superiori, dirigenti o amministratori di sistema
- Le password non devono essere scritte o memorizzate in modo improprio (ad esempio in Excel) a meno che il reparto IT non abbia approvato un metodo sicuro (ad es. uno strumento per password) allo scopo
- La password deve essere cambiata a intervalli regolari
- Le password devono essere cambiate se vi sono indicazioni che siano state rese pubbliche, ovvero rese accessibili a terzi
- Segni di uso improprio devono essere segnalati immediatamente al reparto IT responsabile
- Se un utente ha un account utente dedicato con privilegi amministrativi, non può essere utilizzata la stessa password dell'account standard
- Il titolare dell'account è, in ogni caso, responsabile del rispetto della politica sulle password, anche se non è tecnicamente richiesta. In nessun caso possono essere utilizzate password standard, vuote o deboli

3 Politica sulle password

3.1 Definizione

Per raggiungere un livello appropriato di sicurezza delle informazioni, vengono applicate diverse politiche sulle password in base ai privilegi richiesti. Viene fatta una distinzione tra:

- utilizzo generale di tipo «Utente» senza privilegi amministrativi su sistemi ICT
- utilizzo specifico di tipo «Amministratore» con privilegi amministrativi su uno o più sistemi ICT. Gli account utente di tipo «Amministratore» si distinguono in:
    - account di servizio / di sistema / di assistenza (utilizzati per funzioni automatizzate, installazione o gestione di componenti in sistemi ICT come ad es. OS, database, applicazioni o account di rete ecc.)
    - account amministratore (utilizzati per le singole persone per dare loro accesso privilegiato ai sistemi ICT)

3.2 Gestione delle password

1. La password è assegnata a un ID di account unico (utente o amministratore)
2. Come l'ID dell'account, anche la password è personale. La password è nota solo alla persona responsabile.
3. La password non deve essere salvata come testo in chiaro
4. La validità della password non deve mai superare i 360 giorni o 540 giorni (vedere capitolo 3.3)
5. Una nuova password verrà rifiutata se è presente tra le ultime 5 password utilizzate
6. Il numero di tentativi falliti di inserimento della password è limitato a 6. Dopo il sesto tentativo, l'account verrà bloccato finché un amministratore non lo sbloccherà di nuovo.
7. Il contatore dei tentativi falliti di accesso non deve essere azzerato in meno di 60 minuti
8. Le password temporanee possono avere una validità di <72 h e l'utente deve essere invitato a cambiare la password temporanea al primo accesso. Questo vale se tecnicamente fattibile. In caso contrario, ogni titolare dell'account è responsabile della modifica della propria password
9. L'assegnazione automatica della password all'apertura di un account utente viene eseguita secondo le stesse linee guida

Regolamento speciale per account di servizio / di sistema / di assistenza:

- eccezione alla regola n. 2: le password associate a questo tipo di account possono essere conservate in uno strumento per password sicuro (criptato) con accesso protetto da password e condivise con più persone attraverso gruppi di ruoli e permessi definiti, se ciò è necessario per svolgere la propria attività
- eccezione alla regola n. 4: le password associate a questo tipo di account possono avere, se necessario, l'opzione password senza scadenza abilitata
- eccezione alla regola n. 6: le password associate a questo tipo di account non devono essere bloccate automaticamente

La gestione delle eccezioni è reperibile al capitolo 3.5.

3.3 Disposizioni per le password

La password per un account di tipo **«Utente» senza** privilegi amministrativi sui sistemi ICT deve soddisfare i seguenti requisiti:

- Contiene almeno 12 caratteri per una validità della password di 360 giorni o almeno 16 caratteri per una validità di 540 giorni
- Ha una complessità di 4 su 4, il che significa che i seguenti caratteri devono essere usati almeno una volta:
  - lettere maiuscole
  - lettere minuscole
  - numeri 0–9
  - punteggiatura o caratteri speciali (non tutti i sistemi ICT accettano tutti i caratteri)
- Non deve contenere il nome dell'account
- Non deve contenere numeri nella prima e nell'ultima posizione
- Non deve contenere 3 caratteri identici consecutivi

Per le password di un account del tipo **«Amministratore» con** privilegi amministrativi sui sistemi ICT, si applicano le seguenti regole speciali aggiuntive:

Regolamento speciale per account di servizio / di sistema / di assistenza:

- Contiene almeno 32 caratteri
- La password deve essere generata in modo casuale e documentata utilizzando uno strumento per password adeguato (vedere eccezione alla regola n. 2, capitolo 3.2)

Regolamento speciale per gli account amministratore:

- Contiene almeno 15 caratteri

Regolamento speciale per i sistemi di terzi (B2C / B2B e altri) gestiti dal gruppo Arbonia:

Le disposizioni per le password si applicano anche ai sistemi di terze parti, ma possono essere adattate, se necessario, al rispettivo Business Use Case. In ogni caso, i regolamenti speciali devono essere trattati secondo il capitolo 3.5.

Disposizioni speciali per account di Windows – internamente ad Arbonia e applicate automaticamente:

- La nuova password impostata non deve essere presente in un database di password compromesse. Un controllo tecnico durante l'impostazione della password impedisce che questo accada
- La nuova password impostata non deve apparire in un dizionario definito dall'utente. Questo dizionario viene gestito centralmente e include, tra le altre cose, il nome dell'azienda. Le parole non consentite vengono visualizzate direttamente in caso di hit
- La password deve essere modificata se si trova in un database di password compromesse

3.4 Strategia relativa alle password

Cronologia delle password	5
Validità massima della password	360 (12–15 caratteri) o 540 giorni (≥16 caratteri)
Lunghezza massima della password	0
Complessità	4/4 (lettere maiuscole / minuscole / numeri 0–9 / punteggiatura o caratteri speciali)
Lunghezza minima della password o Utenti o Account di servizio / di sistema / di assistenza o Account amministratore	 12 caratteri 32 caratteri (generata in modo casuale) 15 caratteri
Crittografia inversa (dominio Windows)	disattivata
Numero di tentativi di accesso falliti fino al blocco dell'account	6
Durata del blocco dell'account	Finché un amministratore non lo sblocca
Durata fino al ripristino del contatore dei tentativi di accesso falliti	≥ 60 minuti
Disposizioni speciali (dominio Windows)	La password non deve contenere numeri nella prima e nell'ultima posizione La password non deve contenere 3 caratteri identici consecutivi

3.5 Eccezioni / disposizioni speciali

Tutte le procedure di autenticazione informatica attuano e verificano, per quanto possibile, il rispetto dei requisiti della presente politica. Se mancano i presupposti tecnici per l'implementazione, questi devono essere assicurati attraverso un processo manuale dal rispettivo titolare dell'account e deve essere usata una password forte nell'ambito delle possibilità del sistema.

Il responsabile della sicurezza IT locale può concedere deroghe a questa politica se vengono rispettati i principi di sicurezza delle informazioni e non vi è alcun rischio per i sistemi ICT del gruppo Arbonia. Quest'ultimo decide, se necessario in consultazione con il responsabile della sicurezza ICT, se concedere un'eccezione o definire ulteriori misure per ridurre al minimo il rischio. Tutte le eccezioni devono essere registrate per iscritto in un registro.

4 Creazione di password forti

Ci sono diverse tecniche per creare e ricordare una password forte:

Esempio 1: creare una password forte basandosi su una frase

Scegliete una frase che potete ricordare facilmente e trasformatela in una password.

Es.: Non è poi così difficile scegliere una password forte.

Utilizzate le prime lettere o più lettere delle singole parole e arricchite la password con numeri e caratteri speciali.

Es.: Nèpcdiffs1Pf.

Esempio 2: creare una password forte sostituendo i caratteri

Scegliete una parola che riuscite a ricordare facilmente, ad esempio «pomeriggio» e definite una sequenza speciale di caratteri, ad es. «1$1». Ora sostituite le parti definite / lettere della parola con la sequenza speciale di caratteri per ottenere una password forte.

Es.: Pomer1$1gg1$10

Si prega di notare che non si dovrebbero mai utilizzare informazioni liberamente disponibili sui social media per creare la propria password. Ulteriori suggerimenti sulla sicurezza delle password sono disponibili nei nostri corsi di formazione sulla consapevolezza della sicurezza informatica.

5 Documenti di riferimento

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Direttiva per l'utilizzo dei sistemi IT in Arbonia

6 Entrata in vigore

Cognome	Unità commerciale	Funzione	Data	Firma
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-07-08	n/a

7 Allegati rilevanti

N.	Descrizione	Nome del file
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	