CEDIT Srl
V.le Brodolini, snc
84091 Battipaglia (Sa)
Tel 0828 302689 - Fax 0828 614326
www.ceditweb.com | info@ceditweb.com
P.Iva 04565550656

MISURE MINIME DI SICUREZZA

In riferimento alla nota MIUR n. 3015 del 20/12/2017 avente ad oggetto “Misure minime di sicurezza ICT per le pubbliche amministrazioni”, il presente documento descrive la policy della Cedit srl in materia di sicurezza informatica, inerente al solo software Myeschool, in uso presso le scuole fruitrici e licenziatarie, delle procedure informatiche commercializzate dalla medesima società.

A seguire si evidenziano i capitoli estratti dal questionario dell'AgID, compilati nelle parti di competenza riguardanti la società Cedit :

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Tutti i sistemi Cedit, sono gestiti direttamente dalla società con i propri tecnici qualificati ed identificati. I prodotti Cedit, consentono per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile, la profilatura di ciascun utente avviene tramite un sistema puntuale di permessi e profili, al fine di gestire i privilegi per ogni funzionalità del software.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Ogni accesso al sistema Myeschool viene automaticamente registrato. Tutte le operazione effettuate dagli utenti vengono salvate in file di log, il cui accesso è reso disponibile a qualsiasi richiesta proveniente dall’utente autorizzato o dalle autorità preposte.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Vedi punto 5.1.1M
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Il sistema Myeschool registra su tabella di log ogni singola operazione effettuata sui dati, la medesima poi viene storicizzata ogni mese.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative,	Il sistema Myeschool consente in ogni istante, lato amministratore

				garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	di sistema, di verificare lo status delle utente e relativi accessi attraverso le proprie ACL (lista di controllo degli accessi), che consente di verificare anche la data dell'ultimo accesso.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Nei log vengono regolarmente tracciate (all'interno del file LOG) tutte le modifiche alle utenze del sistema Myeschool.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Il sistema Myeschool incoraggia questa best practice, dando anche indicazioni, ma la sua applicazione è lasciata all'Istituto
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Il sistema Myeschool incoraggia questa best practice, dando anche indicazioni, ma la sua applicazione è lasciata all'Istituto
5	7	3	M	Assicurare che le credenziali delle utenze amministrative	Il sistema Myeschool incoraggia questa best practice, dando anche

				vengano sostituite con sufficiente frequenza (password aging).	indicazioni, ma la sua applicazione è lasciata all'Istituto
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Il sistema Cedit incoraggia questa best practice, dando anche indicazioni, ma la sua applicazione è lasciata all'Istituto
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Myeschool associa agli utenti amministratori profili particolari a cui solo, sono permesse determinate operazioni.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Nel sistema Myeschool, ogni utenza è legata ad una singola anagrafica del personale.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono	

				essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate all'interno della base dati il cui accesso è consentito solo a specifici applicativi Myeschool.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Myeschool effettua automaticamente con cadenza programmata il backup dei dati ed del sistema per consentire in qualsiasi momento il ripristino del servizio. Nello specifico viene effettuato: - Backup dei log ogni 6 ore - Backup del db ogni 2 ore, - Backup completo alle ore 20 di ogni giorno
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Il sistema Myeschool, per la natura della sua architettura, può essere ripristinato in qualsiasi momento su web server Linux o Windows, i tempi di ripristino dal Faul completo sono di circa 4 ore.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Vedi punto ABSC 10.1.1
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Le procedure generali di ripristino dei server vengono verificate ogni settimana.

CEDIT Srl
V.le Brodolini, snc
84091 Battipaglia (Sa)
Tel 0828 302689 - Fax 0828 614326
www.ceditweb.com | info@ceditweb.com
P.Iva 04565550656

10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Tutti i dati ritenuti sensibili dei server Myeschool sono cifrati e protette da protocollo HTTPS,prima di essere trasferiti ai repository di backup
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Le copie dei dati dei server Myeschool vengono mantenute su differenti data center dislocati su reti geografiche differenti.

CEDIT Srl
l'Amministratore