## Assessment Moderate

### Access Control

* **AC-2(1): ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT** 
  + L’organizzazione impiega meccanismi automatizzati per supportare la gestione degli account del sistema
    - **Tale funzionalità non è implementata, ma sarebbe possibile inviare una notifica a seguito dell’eliminazione di un account.**
* **AC-2(2) :ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS** 
  + Il sistema informativo deve automaticamente rimuovere account temporanei/di emergenza dopo un intervallo di tempo definito dalla organizzazione
    - **Tale funzionalità non è implementata in quanto non è stato previsto l’uso di account temporanei / di emergenza.**
* **AC-2(3) :ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS** 
  + Il sistema informativo disabilita automaticamente account inattivi dopo un certo periodo di tempo stabilito
    - **Tale funzionalità non è implementata. Si potrebbe implementare tuttavia una serie di controlli automatici**
* **AC-2(4) :ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS** 
  + Il sistema informativo realizza automaticamente la valutazione per la creazione di account, la loro modifica, l’abilitazione, la disabilitazione e la rimozione, nonché le notifiche del personale.
* **AC-4 : INFORMATION FLOW ENFORCEMENT** 
  + Il sistema informativo fa l’enforcement di autorizzazioni approvate per controllare il flusso delle informazioni all’interno del sistema e tra i sistemi interconnessi in base al flusso di controllo stabilito dall’organizzazione
    - **Il sistema gestisce l’autorizzazione delle informazioni interne ed esterne in ingresso al sistema stesso, così come in accordo alle policy stabilite**
* **AC-5: SEPARATION OF DUTIES** 
  + L’organizzazione separa i vari compiti che spettano ai singoli individui, ne separa dunque i doveri e definisce le autorizzazioni di accesso del sistema al fine di supportare la separation of duties
    - **Il sistema separa i vari compiti che spettano ai singoli individui, nonché i doveri. Avendo solo due tipologie di utenti, la distinzione è netta in termini di autorizzazione, ed è quindi implementata.**
* **AC -6: LEAST PRIVILEGE**
  + L’organizzazione implementa il criterio del privilegio minimo, al fine di fornire le autorizzazioni e i privilegi minimi per permettere ad un dato utente di adempiere alle proprie funzionalità
    - **Il sistema prevede di assegnare ad ogni utente solo i permessi che gli sono strettamente necessari. L’amministratore della web app ha infatti i permessi necessari a modificare solo quanto gli compete. Gli utenti della web app hanno i permessi necessari al normale utilizzo della web app e possono modificare solo gruppi e liste che gli appartengono.**
* **AC-6(1): LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS** 
  + L’organizzazione autorizza esplicitamente l’accesso a funzionalità di sicurezza, sviluppate in hardware o software, per accedere ad informazioni protette.
    - **Le funzionalità di sicurezza sono disponibile solamente all’Amministratore e non agli utenti normali.**
* **AC-6(2): LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS** 
  + L’organizzazione richiede che gli utenti degli account del sistema, con un determinato ruolo, e con accesso ad informazioni o funzioni di sicurezza, utilizzino account non privilegiati per accedere ad informazioni non privilegiate
    - **È sicuramente vero che un utente registrato non ha permessi per accedere ad informazioni classificate. Al contempo un amministratore può solo accedere al pannello di amministrazione, ma per usufruire dei servizi non critici dell’utente, dovrebbe a sua volta essere un utente registrato.**
* **AC-6(5): LEAST PRIVILEGE | PRIVILEGED ACCOUNTS** 
  + L’organizzazione restringe gli account privilegiati unicamente a personale con ruolo ben definito nell’organizzazione
    - **Ciò risulta implementato, dato che solo i membri fidati dell’organizzazione accedono ai ruoli d’amministrazione (noi stessi)**
* **AC-6(9): LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS**
  + L’organizzazione proibisce accessi privilegiati a utenti non organizzativi
    - **Questo requisito è soddisfatto in quanto solo membri appartenenti all’organizzazione e fidati, possono rivestire ruoli amministrativi, e quindi privilegiati.**
* **AC - 6(10): LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS** 
  + Il sistema informativo impedisce che utenti non privilegiati eseguano funzioni non privilegiate, come disabilitare o alterare misure di sicurezze
    - **Tale requisito è garantito dal fatto che utenti comuni non hanno accesso ad alcuna informazione o funzionalità di sicurezza che espongano il back-end. Questo sempre assumendo che gli account amministrativi non siano violati**.
* **AC – 11: SESSION LOCK**
  + Il sistema informativo previene ulteriori accessi bloccando la sessione di un utente, a meno che esso non richieda di terminare la sessione. Una volta che l’utente decide di riaccedere, una nuova sessione viene ristabilita e mantenuta.
    - **Non implementato.**
* **AC – 11(1): SESSION LOCK | PATTERN-HIDING DISPLAYS (no use)**
  + Il sistema nasconde tramite il blocco di sessione, informazioni precedentemente visibili tramite immagini pubbliche
* **AC – 12: SESSION TERMINATION**
  + Il sistema termina automaticamente una sessione utente dopo una richiesta dell’utente.
    - **Il sistema chiude la sessione di un utente solo se questo esplicita il log out**
* **AC – 17(1): REMOTE ACCESS | AUTOMATED MONITORING / CONTROL (no use)**
  + Il sistema informativo monitora e controlla metodi di accesso remoto
* **AC – 17(2): REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION (no use)**
  + Il sistema informativo implementa meccanismi di cifratura per proteggere la confidenzialità e l’integrità dell’accesso remoto
* **AC – 17(3): REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS (no use)**
  + Il sistema informativo indirizza tutti gli accessi remoti attraverso un certo numero di punti di controllo della rete.
* **AC – 17(4): REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS (no use)**
  + L’organizzazione autorizza l’esecuzione di comandi privilegiati e accessi a informazioni di sicurezza tramite accessi remoti solo a chi ne necessita e documenta il criterio secondo cui tali accessi avvengono in un piano di sicurezza.
* **AC-18(1):WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION (no use)**
* **AC-19(5): ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION (no use)**
* **AC – 21: INFORMATION SHARING** 
  + Il sistema facilita la condivisione di informazioni permettendo agli utenti di determinare se le autorizzazioni di accesso assegnate al partner di condivisione coincidano con le restrizioni di accesso alla risorsa
    - **Le liste condivise con un gruppo sono visibili solo agli utenti autorizzati a visionare tale gruppo.**

### Identification and authentication control

* **IA -2(2): IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS** 
  + Il sistema informativo implementa più fattori di autenticazione per l’accesso alla rete da parte di utenti non privilegiati
    - **Nella nostra organizzazione non ci sono utenti non privilegiati.**
* **IA – 2(3): IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS** 
  + Il sistema informativo richiede più fattori per l’autenticazione locale di utenti privilegiati
    - **Il sistema implementa solo un fattore di autenticazione per accessi locali privilegiati (amministratori di sistema.)**
* **IA-2(8): IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT** 
  + Il sistema informativo implementa autenticazioni resistenti ad attacchi di replay in caso di accesso di utenti privilegiati
    - **L’autenticazione del webserver non è mutuamente autenticata, ma comunque cifrata su SSL.**
* **IA-2(11): IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE** 
  + Il sistema è in grado di implementare più meccanismi di autenticazione per utenti privilegiati e non, richiedendo una autenticazione tramite un dispositivo, e la seconda per mezzo di un secondo dispositivo
    - **Non è implementato tale requisito.**
* **IA-3 : DEVICE IDENTIFICATION AND AUTHENTICATION (no use)**
  + Il sistema informativo identifica ed autentica univocamente i dispostivi prima di stabilire una connessione
* **IA – 5(2): AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION (no use)**
  + Il sistema informativo realizza una autenticazione basata su PKI, validando i certificati ed eventualmente costruendoli, garantendo solo accessi a chi detiene i certificati distribuiti, associando l’identità del detentore al certificato rilasciato.
* **IA – 5(3): AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION (no use)**
  + L’organizzazione richiede che il processo di registrazione atto a ottenere le credenziali sia condotto in persona o da una terza parte fidata.

### System and communications protection control

* **SC- 2: APPLICATION PARTITIONING** 
  + Il sistema informativo separa le funzionalità utente, incluse interfacce utente, dalle funzionalità di gestione del sistema
    - **Il sistema informativo fornisce determinate viste per l’utente e determinate per l’amministratore.**
* **SC – 4: INFORMATION IN SHARED RESOURCES (no use)**
  + Il sistema informativo previene trasferimenti di informazioni non autorizzate e non previste tramite le risorse condivise di sistema
* **SC – 7(3): BOUNDARY PROTECTION | ACCESS POINTS** 
  + L’organizzazione limita il numero di connessioni esterne al sistema informativo
    - **Tale requisito non è implementato.**
* **SC – 7(4): BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES** 
  + L’organizzazione implementa una interfaccia di gestione per ogni servizio di telecomunicazione e ne stabilisce delle policy di flusso. Bisogna mantenere confidenzialità e integrità nella trasmissione di dati da tali interfacce e documentare ogni possibile eccezione per le policy di flusso
    - **Tale requisito non è implementato in quanto non è prevista una policy di gestione di flussi di informazioni.**
* **SC – 7(5): BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION** 
  + Il sistema informativo impedisce connessioni ad interfacce di default, ma concede solamente connessioni tramite eccezioni (deny all permit exceptions)
    - **Requisito non implementato. Avrebbe poco senso per un webserver, almeno dall’interfacciamento utente. Tuttavia l’accesso al database avviene solo da determinati ip.**
* **SC – 7(7): BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES (no use)**
  + Il sistema informativo, in congiunzione ad un dispositivo remoto, previene il dispositivo dall’accedere contemporaneamente al sistema e trasmettere le informazioni su di una rete esterna
* **SC – 8: TRANSMISSION CONFIDENTIALITY AND INTEGRITY** 
  + Il sistema informativo protegge la confidenzialità e l’integrità delle informazioni trasmesse
    - **Il sistema realizza tale requisito grazie ai protocolli sicuri implementati basati su SSL.**
* **SC – 8 (1): TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION** 
  + Il sistema implementa meccanismi crittografici per prevenire divulgazione non autorizzata di informazioni durante la trasmissione, a meno che non siano protetti attraverso protezioni fisiche alternative
    - **Il sistema realizza tale requisito grazie ai protocolli sicuri implementati basati su SSL.**
* **SC – 10: NETWORK DISCONNECT** 
  + Il sistema informativo termina la connessione automaticamente quando termina la sessione di un utente
    - **Al momento non è implementato questo requisito**
* **SC – 17: PUBLIC KEY INFRASTRUCTURE CERTIFICATES** 
  + L’organizzazione implementa una PKI nella quale emette certificati o ne richiede da altre CA certificate
    - **Il sistema emette certificati e al momento non ne richiede, in quanto la CA è self signed. Tuttavia dovremmo implementare una catena fidata**
* **SC – 23: SESSION AUTHENTICITY** 
  + Il sistema protegge l’autenticità della comunicazione sulla sessione
    - **Il sistema al momento non prevede una doppia autenticazione su webserver (HTTPS), però i protocolli usati garantiscono autenticità sulla comunicazione**

|  |  |
| --- | --- |
|  |  |