Table of Contents

Ex Platform SSP

# Ex Platform overview

This is the frontmatter for the EX System Security Plan

# Control responses and guidance

## ACCOUNT MANAGEMENT (AC.2)

### AC.2.1.10 - AUTOMATED SYSTEM ACCOUNT MANAGEMENT

#### Control Statement

The organization employs automated mechanisms to support the management of information system accounts

#### AC.2.1.10 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned

#### Component: EC-Pol-AC-Auth

Req AC.2.1.10 is implemented properly for Cloud Storage component.

##### Implementation Status: implemented

### AC.2.1.11 - REMOVAL OF TEMPORARY ACCOUNTS

#### Control Statement

The information system automatically disables temporary accounts after 1 day.

#### AC.2.1.11 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned

#### Component: EC-Pol-AC-Auth

Req AC.2.1.11 is implemented using the Access control and authentication procedure for EC-Pol-AC-Auth component

##### Implementation Status: implemented

## ACCESS ENFORCEMENT (AC.3)

### AC.3.1.10 - DUAL AUTHORIZATION

#### Control Statement

The information system enforces dual authorization for organization-defined privileged commands

#### AC.3.1.10 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned

## INFORMATION SYSTEM COMPONENT INVENTORY (CM.8)

### CM.8.2.2 - AUTOMATED MAINTENANCE

#### Control Statement

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

#### CM.8.2.2 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned

#### Component: Cloud Storage

Req CM.8.2.2 is implemented using ITinv tool to maintain an accurate inventory of information for Cloud Storage component.

##### Implementation Status: implemented

## INFORMATION SYSTEM BACKUP (CP.9)

### CP.9.1 - TESTING FOR RELIABILITY

#### Control Statement

The organization tests backup information every 3 months to verify media reliability and information integrity.

#### CP.9.1 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned

#### Component: CMS

Req CP.9.1 is implemented using the Disaster Recovery procedure for the CMS component.

##### Implementation Status: implemented

### CP.9.2 - TEST RESTORATION USING SAMPLING

#### Control Statement

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing

#### CP.9.2 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned

## AUTHENTICATOR MANAGEMENT (IA.5)

### IA.5.1.4 - AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

#### Control Statement

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy requirements.

#### IA.5.1.4 Summary information

#### What is the solution and how is it implemented?

#### Component: This System

##### Implementation Status: planned