RISK MANAGEMENT PLAN # 1

Revision 1 Date: 11/20/2023

Asset Name - ID: Instagram - S1

Priority: Low

A/ Risk Description and Consequences:
Threats: Weak Passwords, Unauthorized Access, Impersonation.
Description: Unauthorized access to the Instagram account due to weak passwords. Mimicking of my identity.
Consequence: Potential reputational damage and loss of control over personal brand.

B/ Mitigation Strategies:
1. Strong Password Policy: Maintain and regularly update a strong password.
2. Multi-Factor Authentication: Implement an additional layer of authentication.
3. Regular Account Activity Check.
4. Enabling Account Recovery Options.

C/ Trip Wires:
1. Unrecognized account activity or login attempts.
2. Notification of potential unauthorized access.

D/ Contingency Actions to take upon identification:
1. Immediately change the password.
2. Review recent account activity for any unauthorized changes.
3. Contact Instagram support for assistance.

E/ Resources needed:
1. Familiarity with multi-factor authentication settings.
2. Contact of Instagram support team.
3. Second email address to enable account recovery.

F/ Notifications
1. Internal notification to the account owner (Myself).
2. External notification to Instagram support.

G/ Subject Matter Expert/Person Responsible for implementing plan:
Fougnigue Sefon

H/ Date Plan Must be Ready:
12/01/2023

I/ Approvals

Fougnigue Sefon
Dr. Jennex

RISK MANAGEMENT PLAN # 2

Revision 1 Date: 11/20/2023

Asset Name - ID: People Work Relationship - Syst001

Priority: High

A/ Risk Description and Consequences:
Threats: Unauthorized Access to Sensitive Work Information, Misinformation or Manipulation of Work-related Data, Disruption in Team Collaboration and Communication
Description: access to data, files, or resources that are confidential or restricted. Intentional or unintentional alteration of work-related data. Complicated or lack of exchange of information and coordination among team members.
Consequence: Compromise of sensitive work information, integrity issues in work-related data, and disruptions in team communication.

B/ Mitigation Strategies:
1. Enable Two-Factor Authentication: Implement an additional layer of authentication for enhanced security.
2. Data Validation Checks: Implement a multi-layered system for data validation checks to ensure the reliability of work-related data.
3. Alternative Communication Platform: Identify and have alternative communication platforms to ensure continuous collaboration.

C/ Trip Wires:
1. Unrecognized access or login attempts to work-related information.
2. Identification of potential misinformation or manipulation in work-related data.
3. Disruptions in Microsoft Teams.

D/ Contingency Actions to take upon identification:
1. Change of password, review of account activity, collaboration with IT department
2. Analyze data validation checks to identify and rectify any misinformation or manipulation.
3. Utilize alternative communication platforms in case of disruptions with the primary platform.

E/ Resources needed:
1. Permission to change passwords and review account activity.
2. Contact of IT
3. Training on Data Validation, Access to Work-Related Systems
4. Identification and testing of alternative communication platforms.

F/ Notifications
1. Internal notification to the account owner (Yourself).
2. External notification to relevant supervisors and IT security personnel.

G/ Subject Matter Expert/Person Responsible for implementing plan:
Fougnigue Sefon
Chari Hill (Supervisor)

H/ Date Plan Must be Ready:
12/01/2023

I/ Approvals
Shawn Fouts (Director)
IT Security Officer