Cyber Security Awareness

Created by

**UPTOWN IT**

by

**<<NAME>>**

**PROJECT REFERENCE:**

**DATE:**

Contents

[PART 1 Establish the current level of cyber security awareness and required awareness program 4](#_Toc108773108)

[Review of Cyber Security Audit Report 4](#_Toc108773109)

[Communication and Feedback – Audit Review and Assessment 5](#_Toc108773110)

[Cyber Security Program Proposal 5](#_Toc108773111)

[Cyber Security Procedure 6](#_Toc108773112)

[Conversation with relevant stakeholder 7](#_Toc108773113)

[PART 2 Support cyber security awareness and organise and review training 8](#_Toc108773114)

[Training Program One (Replace with real name) 8](#_Toc108773115)

[Training Program Two (Replace with real name) 9](#_Toc108773116)

[PART 3 Review cyber security awareness in the workplace 10](#_Toc108773117)

[Review and communicate the latest cyber security threats and trends 10](#_Toc108773118)

[Communication and Feedback – Latest Cyber Security Threats and Trends 10](#_Toc108773119)

[PART 4 Contingency task and cyber security knowledge 11](#_Toc108773120)

[Contingency Task 11](#_Toc108773121)

[Cyber Security Knowledge 11](#_Toc108773122)

[REFERENCES 12](#_Toc108773123)

Remove all blue text once your report is completed.   
The blue text is intended at giving you some pointers for the report content.

DO NOT REMOVE template headings.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | Version | Date Completed | Completed by | Approved by | Date Approved |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# PART 1 Establish the current level of cyber security awareness and required awareness program

To establish the current level of cyber security awareness in the company, review the audit results presented and identify the areas of cyber security identified by the problems reported, the impact on the workplace, the risk level, and an appropriate training priority.

Areas can include but are not restricted to:

* Phishing attacks
* Removable media
* Passwords and authentication
* Physical security
* Working remotely
* Public Wi-Fi
* Social Media Use
* Internet and Email Use
* Social engineering
* Security at home

## Review of Cyber Security Audit Report

Introduction – Write an introduction for this heading

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cyber Security Problem | Cyber Security Area | Workplace Impact | Risk Level  (High, Moderate, Low) | Awareness Training Priority  (1 Highest – 10 Lowest) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Add rows as needed |  |  |  |  |

## Communication and Feedback – Audit Review and Assessment

Introduction – Write an introduction for this heading

Arrange a conversation with a team member and seek feedback regarding your review and assessment of the audit report and the workplace impact.

Document the communication and feedback received.

Evidence of conversation can be oral, verbal, written or visual. For example, an email, a written report, a recorded audio or video.

## Cyber Security Program Proposal

Introduction – Write an introduction for this heading

Propose a set of cyber security procedures to be included in a company-wide Cyber Security Awareness Policy.

Ensure that the procedures proposed cover as a minimum all the problems identified in the audit report.

For each procedure proposed, provide a description of the purpose and content.

|  |  |  |
| --- | --- | --- |
| Proposed Procedure | Purpose | Content Description |
|  |  |  |
|  |  |  |
|  |  |  |
| Add rows as needed |  |  |

## Cyber Security Procedure

Introduction – Write an introduction for this heading

Select one of the procedures proposed above and create the procedure. Use the template provided to write the procedure to ensure compliance with organisational documentation procedures and guidelines.

|  |  |
| --- | --- |
| **UPTOWN IT**  **Cyber Security Awareness Procedure**  **PROCEDURE NAME** | |
| Purpose | Describe the purpose of this procedure in details. |
| Scope | Identify who this procedure applies to in the organisation. |
| Responsibilities | Describe the roles and responsibilities of each position affected by the procedure. |
| Version Control | Naming, numbering and dating conventions used by the organisation to assign version information. |
| Rules/Guidelines | Write detailed instructions for each rule or step. |
| Referenced Documents | Identify other organisational documents referenced in this procedure, e.g., Infrastructure Diagram. |
| Approval | Approval status of the procedure. |
| Review Date | When the procedure is due for review. |

## Cyber security maintenance procedure schedule

Introduction.

Propose a cyber-security procedures maintenance schedule to review procedures on a regular basis. In the proposal, identify the exceptional circumstances that may trigger an out-of-schedule procedure review. The maintenance schedule must consider the volatile nature of cyber security threats.

## Strategies for promoting cyber security awareness

Introduction.

Suggest three (3) strategies for promoting cyber security awareness in the workplace. The strategies proposed must be following organisational policies and procedures.

## Conversation with relevant stakeholder

Introduction.

Arrange a conversation with your manager and seek feedback regarding the following points:

* 1. The suitability of the procedure that you have written. Modify procedure if required. Document the conversation in the Conversation Log.
  2. The proposed maintenance schedule to review cyber security awareness procedures.
  3. Discuss and confirm proposed strategies to promote cyber security awareness amongst employees.

Document discussion and confirmed strategies in the Conversation Log.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Conversation Log | | | | |
| Date | Topic | Discussion | Stakeholder | Medium  Any oral form of communication, e.g., F2F, Zoom and phone call. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  | Add rows as necessary |  |  |

# PART 2 Support cyber security awareness and organise and review training

Introduction – Write an introduction for this heading

After having reviewed the Cyber Security Audit Report provided, you have gathered an understanding of the current staff awareness regarding cyber security. In this task, you need to arrange two (2) training programs. Select the two areas identified in PART 1 as having the highest priority.

Use the Training Program template provided to ensure compliance with organisational documentation procedures and guidelines.

## Training Program One *(Replace with real name)*

|  |  |
| --- | --- |
| **UPTOWN IT**  **Cyber Security Awareness Training program**  **TOPIC NAME** | |
| Referenced Procedure | Procedure or procedures that align with this training plan. |
| Learning Objectives | Describe the leaning objectives of the training program. |
| Recommended Frequency of Training | Organisations may set a recurring timeframe for training or refresher training sessions, e.g., 12 months. |
| Responsibilities | Identify roles and responsibilities of people affected by the training. |
| Topic Overview | Brief Training topic overview. |
| Training Materials  Module 1  Module 2  Module X  … | Write detailed training materials.  Add links to resources as required.  Divide the materials into a number of logical modules  Each module may include some activities and evaluation.  This section must be specific and detailed – Generic information is not acceptable. |
| Activities | General pre-evaluation activities can be provided in this section. Module individual activities can be included in each module. |
| Evaluation | Evaluation criteria and test. |

## Training Program Two *(Replace with real name)*

Introduction – Write an introduction for this heading

|  |  |
| --- | --- |
| **UPTOWN IT**  **Cyber Security Awareness Training program**  **TOPIC NAME** | |
| Referenced Procedure | Procedure or procedures that align with this training plan. |
| Learning Objectives | Describe the leaning objectives of the training program. |
| Recommended Frequency of Training | Organisations may set a recurring timeframe for training or refresher training sessions, e.g., 12 months. |
| Responsibilities | Identify roles and responsibilities of people affected by the training. |
| Topic Overview | Brief Training topic overview. |
| Training Materials  Module 1  Module 2  Module X  … | Write detailed training materials.  Add links to resources as required.  Divide the materials into a number of logical modules  Each module may include some activities and evaluation.  This section must be specific and detailed – Generic information is not acceptable. |
| Activities | General pre-evaluation activities can be provided in this section. Module individual activities can be included in each module. |
| Evaluation | Evaluation criteria and test. |

# PART 3 Review cyber security awareness in the workplace

## Review and communicate the latest cyber security threats and trends

Use reliable and up-to-date sources to research and review the latest cyber security threats and trends affecting the industry. In the light of the review, propose any improvements that would benefit our company. Identify which procedure(s) must be updated to incorporate the new information.

|  |  |  |  |
| --- | --- | --- | --- |
| Cyber Security Threat | Trend | Source(S) | Proposed Improvement & Procedure to Update |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Communication and Feedback – Latest Cyber Security Threats and Trends

Communicate with a team member and seek feedback regarding your review and assessment of the latest cyber security threats and trends and your proposed improvements as presented in 3.1.

Document the communication and feedback received.

Evidence of conversation can be oral, verbal, written or visual. For example, an email, a written report, a recorded audio or video.

# PART 4 Contingency task and cyber security knowledge

Part 4 requires you to carry out research and provide answers to a number of questions. Provide the answers in your own words. Plagiarism is a form of academic misconduct and will not be tolerated. Include references for all your sources using a formal referencing style such as APA or Harvard.

## Contingency Task

Outline the processes that you would follow if a cyber security issue arises that is not covered by the company policies.

## Cyber Security Knowledge

For each item below, identify what would be the cyber security **legislative requirements** and implications**.** Provide examples to illustrate your answers.

1. **Data protection** in Australia
2. **Notifiable Data Breach** in Australia
3. **Cyber security** in international legislation affecting Australia

For each listed policy/procedure, provide the scope of the procedure and three (3) rules or guidelines that should be included to protect the company against cyber security threats.

Provide the answers within the context of the company provided in the scenario.

|  |  |  |
| --- | --- | --- |
| Policy/Procedure For | Scope | Rules/Guidelines  Three (3) for each |
| 1. Securely storing, sharing and managing information |  |  |
| 1. Encryption, and protocols for its uses |  |  |
| 1. Data classification and management |  |  |
| 1. Media/document labelling |  |  |
| 1. Data governance |  |  |
| 1. Acceptable use |  |  |
| 1. Bring your own device |  |  |
| 1. Securely storing, sharing and managing information |  |  |

# REFERENCES