# Information Security Training Plan

## INTRODUCTION

* 1. The purpose of this training plan is to describe the steps taken to assess the information security knowledge of [ORGANIZATION] staff members, identify gaps in knowledge, and document a plan to address those gaps.
  2. The [Position Responsible] is responsible for this training plan and its review and update on an annual basis.
  3. [ORGANIZATION] will continuously evaluate the effectiveness of this training plan through benchmarking and compliance with designated security frameworks.
  4. Training will be delivered using a commercially available tool to provide information security training for staff [Training Tool In Use].
  5. This policy applies to all [ORGANIZATION] employees.

## INFORMATION SECURIITY ASSESSMENT

* 1. As a result of [Event That Resulted in Creating Information Security Training Program], this Information Security Training Program was developed to address gaps in the organization’s security knowledge and experience with developing and executing a plan for addressing those gaps.
  2. In [TRANING TOOL IMPLEMENTATION DATE], [ORGANIZATION] adopted the use of [Training Tool In Use]. [Training Tool in Use] can perform an initial security assessment of staff knowledge, to help understand areas where security awareness is lacking. A Security Awareness Proficiency Assessment (SAPA) was completed, that assessed skills and competencies across the following component areas:
     1. Passwords & Authentication
     2. Internet Use
     3. Incident Reporting
     4. Social Media
     5. Mobile Devices
     6. Email Security
     7. Security Awareness
  3. As part of the training plan during the inaugural year of the [ORGANIZATION] Information Security Program, a SAPA was conducted of [ORGANIZATION] staff in [Date of Review]. The results are below.
  4. [Training Tool In Use] then compared the organization’s scores against similar organizations based on industry and size:
  5. Based on the initial SAPA, there is a gap in information security knowledge for the [Gap Areas]. However, overall, [ORGANIZATION] staff have a good understanding [Areas that did well]. The focus of this year’s training plan will be [Training areas focus].

## TRAINING PLAN AND MILESTONES

* 1. To address the gaps noted earlier in section 2 of this plan, [ORGANIZATION] will take a multi-pronged approach towards information security training:
     1. Initial Information Security Awareness Proficiency Assessment upon hire.
     2. Quarterly training will be conducted based on the seven component areas of the SAPA to further bolster the skills and competencies of [ORGANIZATION] staff.
     3. Monthly compliance training will be conducted, geared towards the frameworks described in section 2 of this plan.
  2. This training will be conducted and documented using the [NAME OF TRAINING TOOL] tool.
  3. The training will be conducted between [Training Start Date] through [Training End Date] as outlined in Appendix A.

## Revision History

### APPENDIX A – INFORMATION SECURITY TRAINING SCHEDULE

| **Month/Year** | **Training Type** | **Training Topic** |
| --- | --- | --- |
| July 2022 | Quarterly Information Security Training |  |
| August 2022 | Compliance Training |  |
| September 2022 | Compliance Training |  |
| October 2022 | Quarterly Information Security Training |  |
| November 2022 | Compliance Training |  |
| December 2022 | Compliance Training |  |
| January 2023 | Quarterly Information Security Training |  |
| February 2023 | Compliance Training |  |
| March 2023 | Compliance Training |  |
| April 2023 | Quarterly Information Security Training |  |
| May 2023 | Compliance Training |  |
| June 2023 | Compliance Training |  |