**Security Awareness Program Timeline.**

The organization covers the security Awareness implementation timeline for the organization cybersecurity training plan.

Effective awareness efforts contribute to minimizing human errors and negligence, which are common sources of security breaches. When all employees including third party such as the transit providers are well-informed about security best practices and understand the importance of safeguarding information, the organization becomes more resilient to cyber threats.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| The Awareness Program | Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 | Month 9 | Month 10 | Month 11 | Month 12 |
| Change your system and network Password. | Stop with solid fill |  |  | Stop with solid fill |  |  | Stop with solid fill |  |  | Stop with solid fill |  |  |
| Conduct A simulated Phishing Exercise. |  | Stop with solid fill | | |  |  |  | Stop with solid fill | | |  |  |
| Technology Updates. |  |  |  |  |  | Stop with solid fill |  |  |  |  |  | Stop with solid fill |
| Education and Training. | Stop with solid fill |  |  | Stop with solid fill |  |  | Stop with solid fill |  |  | Stop with solid fill |  |  |
| Remote Work Security. | Stop with solid fill |  |  |  |  |  |  | Stop with solid fill |  |  |  |  |

1. **Change Your System and Network Password.**

Regularly update passwords to enhance security and prevent unauthorized access.

* Use strong passwords with a mix of upper- and lower-case letters, numbers, and special characters.
* Avoid using easily guessable information like names, birthdays, or dictionary words.
* Avoid sharing accounts; each user should have their own credentials.

1. **Phishing and Social Engineering.**

Educating employees about phishing emails, social engineering tactics, and how to identify suspicious communications is a core aspect of infosec awareness.

* Employees are educated about the risks of clicking on links or downloading attachments from unknown sources.
* Employees are cautioned against responding to urgent requests for sensitive information without verifying the sender's identity through a separate communication channel.

1. **Technology Updates.**

Awareness programs inform employees about the importance of keeping their software, devices, and applications up to date to address vulnerabilities.

1. **Education and Training Awareness.**

The infosec department is responsible for designing and delivering educational programs that raise awareness about information security risks, threats, and vulnerabilities. Training sessions can cover topics such as phishing awareness, password hygiene, data protection, and secure remote work practices.

1. **Remote Work Security.**

With the rise of remote work, employees need to be educated about secure remote work practices, including the use of VPNs, secure Wi-Fi, and protecting sensitive data outside the office environment.