| EXEMPLAR | | | |
| --- | --- | --- | --- |
| **Qualification code:** | 22334VIC | **Qualification title:** | CERTIFICATE IV IN CYBER SECURITY |
| **Unit code:** | VU21995 | **Unit title:** | Manage the security infrastructure for the organisation |
| **Department name:** | BDIT, Computer and Information Technology |  | Enter CRN number |

1. **Cyber Hygiene Checklist Exemplar**
   1. **Cyber Hygiene Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **NO.** | **CHECKLIST ITEM** | **PERFORMED (tick box)** | **NOT PERFORMED (tick box)** |
| **1** | All computers have anti-virus installed that is automatically kept up to date |  | N |
| **2** | All computers have their operating systems automatically updated |  | N |
| **3** | Staff receive cyber awareness training once per year |  | N |
| **4** | All computers are protected with strong passwords |  | N |
| **5** | All administrator accounts on computers are restricted for special need purposes | Y |  |
| **6** | Edge router remote access default username, password and IP address have been changed | Y |  |
| **7** | Wireless network access is configured with WPA2 security and strong password |  | N |
| **8** | Guest wireless network access is on a separate subnet |  | N |
| **9** | All company data is backed up daily offline and offsite (minimum) |  | N |
| **10** | Backup restoration process is tested once a month (minimum) |  | N |
| **11** | AAA is performed on all user logins | Y |  |
| **12** | Logging is compiled from all networking and networked devices. |  | N |
| **13** | Incident response plan has been developed for the company and implemented |  | N |
| **14** | Yearly reports are compiled on the state of company security |  | N |
| **15** | Company network is appropriately segregated to limit unnecessary access |  | N |
| **16** | Company has policies and procedures document written focused on cybersecurity |  | N |
| **17** | Company use reputable cloud services |  | N |
| **18** | Phishing all workforce, including upper management, is regularly performed |  | N |
| **19** | Company has mandated Multi-factor authentication |  | N |
| **20** | Internal controls / access controls implemented | Y |  |
| **21** | No outdated or unsupported software is checked and verified |  | N |
| **22** | Encryption is employed for sensitive data |  | N |
| **23** | Third party security risk management program is employed |  | N |
| **24** | Firewall, intrusion detection, and intrusion prevention systems are employed |  | N |
| **25** | Company has employed Managed service provider or managed security services provider |  | N |
| **26** | Company is Cyber risk insured |  | N |
| **27** | Security Patches Management Policy implemented (All devices are appropriately patched) |  | N |

**Cyber Hygiene Company Score**

4/26 \* 10 = **1.5 *refer to score calculation below***

* 1. **Score Calculation**

After assessment is taken, the following calculation is used to determine the cyber hygiene rating.

Number of items ‘complete’ / 26 \* 10 = Cyber Hygiene Rating

Eg. 4 items complete  
 4 / 26 \* 10 = 1.5 Cyber Hygiene Rating = 1.5

* 1. **Score Assessment**

**Cyber Hygiene Rating 0-4(inclusive)**  
The company must immediately rectify their cyber security posture and improve their score.

**Cyber Hygiene Rating 5-7 (inclusive)**The company must rectify their cyber security posture within 12 months and improve their score

**Cyber Hygiene Rating 8-10 (inclusive)**The company cyber security posture is adequate.