**PART 1 –INFORMATION ASSET INVENTORY AND RANKING**

**TABLE 1 - LISTING OF INFORMATION ASSETS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Asset** | **Component/ Media** | **Data Owner** | **Type of Sensitive Data** | **RTO** | **RPO** |
| 1. AD Service | Desktop Server A SaaS  Database | CIO | PII  CUSTOMER CONFIDENTIAL | 8hours | 4hours |
| 2. AD SQL DB | Desktop Server A NAS1 SaaS | CIO | PII | 1hour | 8hours |
| 3. DNS Service | Desktop Server A SaaS | CIO | CUSTOMER CONFIDENTIAL | 30 minutes | 4 hours |
| 4. DNS SQL DB | Desktop Server A NAS1 SaaS | CIO | CUSTOMER CONFIDENTIAL | 1 hour | 4 hourss |
| 5. Exchange email app. | SaaS  Desktop/Laptop | CIO | CUSTOMER CONFIDENTIAL | 30 minutes | 24 hours |
| 6. Email DB | SaaS  Desktop/Laptop  Internal & External Networks | MM  HR | CUSTOMER CONFIDENTIAL  PII | 2 days | 1 week |
| 7. NAS1 App.(Email App) | SaaS  Desktop/Laptopp  Server A | MARKETING DEPARTMENT  CIO | PII  CUSTOMER CONFIDENTIAL | 24 hours | 1 week |
| 8. NAS1 Data | Server A  Disk Array 1 | CIO  MM | CUSTOMER CONFIDENTIAL  PPI | 2 days | 1day |
| 9. NAS2 App. (Company App) | Server B  Disk Array 2 | CIO  CEO | PII | 1 hour | 4 hours |
| 10. NAS3(Company Website) | Server C | CEO | PII | 30 minutes | 4 hours |
| 11. CM DB | Server A,B&C | CIO | PII | 24 hours | 2 days |
| 12. Anti-Spam Software | SaaS  Desktop/Laptop  Server A  NAS1 | CIO | CUSTOMER CONFIDENTIAL | 8 hours | 4 hours |
| 13. Firewall Software | Networks & Network devices  SaaS | CIO | CUSTOMER CONFIDENTIAL  PII | 24 hours | 8 hours |
| 14. PKI services | Desktop/Laptop  SaaS | CIO  Shareholders  CEO | CUSTOMER CONFIDENTIAL | 8 hours | 4 hours |
| 15. Proxy services | Servers A,B,&C  Desktop/Laptop | CIO | PII | 30 minutes | 4 hours |
| 16. Router service | Desktop/Laptop  Server A  Server B  Server C  External & Internal Networks | CIO | CUSTOMER CONFIDENTIAL | 8 hours | 4 hour |
| 17. Security Software | Desktop  Server A  Server B  Server C  SaaS | CIO | PII | 2 days | 1 day |
| 18. SNMP service | Servers A,B, &C  Internal Network | CIO | CUSTOMER CONFIDENTIAL | 30 minutes | 4 hours |
| 19. SSL service | Desktop/Laptop  Internet Network | CIO | PII | 30 minutes | 4 hours |
| 20. TLS service | Desktop/Laptop  Internet Network | CIO | PII | 1 hour | 4 hours |
| 21. SSID service | Desktop/Laptop  Internet Network | CIO | PII | 30 minutes | 4 hours |
| 22. VPN service | Desktop/Laptop  Internet Network | CIO | PII | 30 minutes | 4 hours |
| 23. WAP service | Mobile Phones  Laptop/Desktop  SaaS  Internet Network | CIO | PII | 30 minutes | 4 hours |

Table 2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria 🡺** | **Availability** | **Confidentiality** | **Integrity** | **Capability** | **Vulnerability** | **Total** | **Importance** |
| **Criteria Weight🡺**  **🡻Asset Name** | **High** | **Very High** | **Medium** | **Low** | Very Low |  |  |
| 1. AD Services | 3 | 4 | 4 | 2 | 1 | 2.8 | Important |
| 2. AD SQL DB | 4 | 2 | 2 | 5 | 1 | 2.8 | Important |
| 3. DNS Service | 5 | 3 | 3 | 4 | 4 | 3.8 | Very Important |
| 4. DNS SQL DB | 3 | 2 | 4 | 4 | 4 | 3.4 | Important |
| 5. Exchange email app. | 5 | 4 | 4 | 3 | 3 | 3.8 | Very Important |
| 6. Email DB | 5 | 5 | 3 | 4 | 5 | 4.4 | Very Important |
| 7. NAS1 App. | 1 | 5 | 2 | 3 | 2 | 2.6 | Important |
| 8. NAS1 Data | 4 | 2 | 3 | 4 | 5 | 3.6 | Very Important |
| 9. NAS2 App. (Company App) | 5 | 3 | 4 | 4 | 5 | 4.2 | Very Important |
| 10. NAS3(Company Website) | 5 | 5 | 4 | 5 | 3 | 4.4 | Very Important |
| 11. CM DB | 4 | 5 | 4 | 5 | 5 | 4.6 | Critically Important |
| 12. Anti-Spam Software | 3 | 4 | 3 | 3 | 5 | 3.6 | Very Important |
| 13. Firewall Software | 5 | 5 | 5 | 5 | 5 | 5.0 | Critically Important |
| 14. PKI services | 2 | 1 | 1 | 3 | 1 | 1.6 | Somewhat Important |
| 15. Proxy services | 5 | 2 | 1 | 4 | 0 | 2.4 | Somewhat Important |
| 16. Router services | 5 | 5 | 5 | 5 | 5 | 5.0 | Critically Important |
| 17. Security Software | 5 | 5 | 5 | 5 | 5 | 5.0 | Critically Important |
| 18. SNMP services | 2 | 3 | 2 | 4 | 3 | 2.8 | Important |
| 19. SSL services | 5 | 5 | 5 | 5 | 5 | 5.0 | Critically Important |
| 20. TLS services | 4 | 3 | 4 | 3 | 0 | 2.8 | Important |
| 21. SSID services | 5 | 0 | 1 | 3 | 0 | 1.8 | Somewhat Important |
| 22. VPN services | 5 | 3 | 3 | 5 | 0 | 3.2 | Important |
| 23. WAP services | 5 | 5 | 4 | 5 | 1 | 4.0 | Very Important |

Title: Responsible and Good Use of Organizational Networks, Hardware, and Internet Services

Classification: Internal and External Use Only

Statement of Policy

This security policy describes regulations the employees of Venture Tulip Marketing and Supplies Inc. should abide by while using its computers and network and internet technologies. The policy covers but is not limited to the company’s website, application, Wi-Fi, hardware, and software. The policy is meant for all the authorized users in the organizational structure all the way from the CEO to the sales representatives of Venture Tulip Marketing and Supplies Inc. as well as potential and existing customers of the organization. Users granted access to the assets are required to abide to all the regulations attached to the use of the assets.

Appropriate Use

WI-FI

The management through the CIO allocates computers and laptops to internal users, the employees, with prior approval. They are permitted to use the company’s WI-FI to execute their online-related duties including social media marketing, website access, and creating application awareness to customers. On the other hand, customers are allowed to use the WI-FI while at the premises while seeking services such as logging into the company’s website and application to navigate a particular service. To ensure appropriate protection of privacy, all wireless transmissions will be secured utilizing strong mutual authentication and encryption. Customers will only access WI-FI with the help of the IT technicians who are restricted not to disclose the passwords for the wireless connection. On the other hand, each department will have its WI-FI logins and different levels of restrictions. When establishing a connection to a public hotspot or WLAN within their homes laptop users must use a VPN connection established and used in conjunction with the company’s approved personal firewall service. Internet users are prohibited access to non-work-related platforms such as entertainment websites, for instance, YouTube, sports and gaming sites, and DIY platforms. Users MUST not in any way try to alter authentication of set WI-FI login details. Users aren’t allowed to use the company’s internet to commit cybercrimes including hacking the firm’s websites or applications.

Hardware

Venture Tulip Marketing and Supplies Inc. has computers and laptops and allocates them to employees according to their hierarchy and amount of responsibilities. All department managers and the CEO are assigned laptops and external hard drives with company data relating to their respective departments which they can carry home. Other employees access the websites, company data, and applications using desktops at the company and are not allowed to carry and use the systems anywhere else apart from where they are installed. They are also allowed to use tablets and phones to strictly access the internet for work-related businesses. Clients are prohibited from using the company’s computers and can only access the internet using their gadgets. Employees are not allowed to use personal external storage devices on the company’s gadgets and are not allowed to store non-company data in the desktops and external storage assets of the company. Users are vetoed to using the company’s hardware to store criminal information.

Emails

At no time are email users allowed to send emails with offensive messages relating to issues such as racist statements, abuse, and pornographic content. Employees with company emails are not allowed to disclose secrets of the organizations to competitors and clients. They should also stick to marketing the company using their assigned email accounts and not promote other competitive organizations. Users are also barred from sending mails with the aim to distribute viruses and spam content. Each user is assigned personalized authentication details and has a right to privacy and the CIO is responsible for making sure the Email database is exclusively secret not to disclose personal information to outside sources and parties. Users in the Marketing department are prohibited to disclose the personal information of clients through Email.

System Management

The Chief Information Officer of Venture Tulip Marketing and Supplies Inc. is responsible for the configuration of all access points are configured with proper settings as defined by the WI-FI System-Specific Policy.

They should ensure all computers are encrypted and authenticated appropriately for the effective functioning of the internet connections. The end users, employees, and customers should ensure their desktops and laptop remains properly configured as defined by the workstation standards of the enterprise. This can comprise the configuration of the network interface cards and wireless supplicants. The company’s security software will be responsible for developing the required compliance programs and defining encryption and authentication requirements.

The CIO will monitor employee and customer activities including browsing history and email details to trace any breeches of internet and website use rules and regulations. The company’s security software will also ensure Venture Tulip Marketing and Supplies Inc.’s internet resources, desktops, app, and website are free from viruses to prevent system failures. The company will also outsource auditing solutions for its internet resources and hardware components whether they are operated within the stipulated guidelines and rules.

Violations of Policy

If there are reported or found out cases of prohibited use of WI-FI, Emails, and hardware, Venture Tulip Marketing and Supplies Inc. reserves the right and responsibility to take all the required measures and steps agreed by the top-level management and the company’s disciplinary committee for the specific case. The implications could include business contract termination of the responsible business partner or termination of employment. If the case is beyond the threshold of the only termination of contracts, then the company has a legal right to sue the accused individual or parties. The company can also prevent a dictatorial form of managing clients and employees by developing guidelines for action including a first-time warning for violators and formal notices in workers’ personnel file for additional occurrences.

All violations of this policy should be reported directly to the Company’s HR manager who will forward the matter to the IT department and the CEO for review and legal steps.

Policy Review and Modification

This policy will be assessed by the IT Department- Security section of Venture Tulip Marketing and Supplies Inc. on a half-yearly and annual basis. It can also be reviewed when emergencies such as abrupt changes in technology and ICT objectives of the company. The CIO will also initiate a review when the end users raise issues about the existing policy, modifying it where appropriate. The modification

7. Liability Limitations

Venture Tulip Marketing and Supplies Inc. assumes no liability for unauthorized actions that infringe state, local, or federal laws and regulations. If such an incident occurs, Venture Tulip Marketing and Supplies Inc. will terminate its relationship with the violator who may be its customer or employee with immediate effect. The company will afterward provide no legal protection or assistance for the said party.