Terms of using Flip Robo Technologies

Data It is the responsibility of Flip Robo Technologies employees, interns, vendors and agents with remote access privileges to Flip Robo Technologies corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Flip Robo Technologies.

A. Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong passphrase see the Password policy.

2. At no time should any Flip Robo Technologies employee provide their login or e-mail password to anyone, not even family members.

3. Flip Robo Technologies employees and interns with remote access privileges must ensure that their owned or personal computer or workstation, which is remotely connected to Flip Robo Technologies' corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. Flip Robo Technologies employees and interns with remote access privileges to Flip Robo Technologies' corporate network must not use other than their registered email address, or other external resources to conduct business, thereby ensuring that official business is never confused with personal business.

5. Routers configured for access to the Flip Robo Technologies network must meet minimum authentication requirements.

6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

7. Non-standard hardware configurations must be approved by the IT department, and Flip Robo Technologies must approve security configurations for access to hardware.

8. All PCs, laptops and workstations that are connected to Flip Robo Technologies internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

9. Personal equipment that is used to connect to Flip Robo Technologies networks must meet the requirements of Flip Robo Technologies -owned equipment for remote access.

10. Individuals who wish to implement non-standard Remote Access solutions to the Flip Robo Technologies production network must obtain prior approval from the IT department.

B. DATA SECURITY POLICY

1. Report lost or stolen mobile computing and storage devices to the IT department.

2. Non-departmental owned devices that may connect to the Flip Robo Technologies network must first be approved by the IT department.

3. Compliance with the Remote Access policy is mandatory.

Connectivity

Approved Flip Robo Technologies employees intern and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a user-managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating, installing any required software, and paying associated fees. '

Requirements

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Flip Robo Technologies internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by Flip Robo Technologies IT department.

6. All computers connected to Flip Robo Technologies internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.

7. VPN users will be automatically disconnected from Flip Robo Technologies network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not Flip Robo Technologies - owned equipment must configure the equipment to comply with Flip Robo Technologies VPN and Network policies.

10. Only Flip Robo Technologies - approved VPN clients may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Flip Robo Technologies network, and as such are subject to the same rules and regulations that apply to Flip Robo Technologies - owned equipment, i.e., their machines must be configured to comply with Flip Robo Technologies Security Policies.

C. Employee Termination Removing access

An employee's or Interns credentials shall be inactivated immediately upon termination of employment. This includes, but is not limited to the following:

- Flip Robo Technologies database
- Workstation access
- E-mail access
- Remote access to Flip Robo Technologies network
- VPN client access
- Any other access to Flip Robo Technologies network or programs

D. Leave Policy

• You are entitled to 1 Casual Leave and 1 Sick Leave in a month.

• This internship demands a full-day contribution on Saturdays and Sundays. Other than this you need to devote 3-4 hours daily.

• Your Week off will be on Tuesday and Wednesday.

• You need to inform your reporting manager a week in advance of any planned casual leaves and this needs to be uploaded on the Leave management system as well.

• In order to avail of sick leaves necessary documents need to be submitted to your reporting manager whenever asked.

• Any unplanned leave during the course of Internship will affect your candidature

Please note that no Casual Leave is allowed in the first month of the Internship.