# Treefrog Cybersecurity Policies

*Cybersecurity or information security policies should apply to all employees, executives and contractors. HR and IT departments have special responsibilities with regard to enforcement.* ***Ensure all employees are conversant with security policies in this document and they are reviewed and signed annually.***

## DAY ONE: Train People On

- [ ] What a Strong Password (Passphrase!) looks like.
- [ ] How Phishing works and how to avoid falling victim.
- [ ] How to use a VPN from home.
- [ ] Which WiFi to use and not use (and what a Man-in-the-Middle attack is).
- [ ] What should and should not be downloaded (nothing).
- [ ] Where and how individual backups work.
- [ ] How and where posting images is acceptable.
- [ ] When NOT to send critical data (e.g. from the airport).
- [ ] How NOT to transfer information (e.g. a USB Drive).
- [ ] How and when to update and add software to corporate devices.

## ANNUALLY: Have All Employees Agree

- [ ] Employees should notify IT immediately of any **unusual behaviour** of their hardware, software, or mobile devices. (Slowness, Button Actions)
- [ ] Employee and visitor personal devices should be connected only to the **Guest WiFi** without explicit permission.
- [ ] Checking personal email and internet browsing for **personal reasons** should be done from **personal devices** while connected to the **Guest WiFi**.
- [ ] The rule of **Least Privilege** must be enforced: employees should not have access to more data than they need to do their jobs. Review privileges annually, and explain why this is important.
- [ ] Employees should **never add software to company systems** unless the applications are approved in advance by IT.
- [ ] Employees must agree to follow the patching and upgrade rules set by IT, such as installing updates within a reasonable time period. Otherwise, patches will be done for you by force, for everyone's safety.
- [ ] Employees should be aware of the need to purge sensitive information when it is no longer needed. IT should be empowered to follow the "three Ps" of data: **protect** what is necessary to the business; **push off-line & encrypt**

data which is sensitive but must be saved, and **purge** all data which is no longer needed by the business which will incur liability if it is stolen.

- [ ] Employees should be prohibited or discouraged from lending company computing devices to others.
- [ ] Employees should understand that the loss of sensitive data which is unencrypted is considered a data breach. No sensitive data should leave the premises in any format unless it is encrypted, nor should it be emailed outside the company (even to a personal email account) without being encrypted.
- [ ] Sensitive data should also be encrypted within the company.
- [ ] Devices containing sensitive data should never be left exposed or unattended; they should **require complex passwords**.
- [ ] Remote users should log in via **VPN** or other secured system.
- [ ] Employees should understand the benefits of **two factor authentication** for email and network access.
- [ ] **Password Policy:** strong passwords should be required which are re-set every 90 days; shared passwords should not be allowed.
- [ ] **Password manager applications are recommended** in cases where group company passwords are necessary (building entry for example); this will allow for changes if members of the group leave the company.
- [ ] Employees should consider adding **anti-malware software** to any personal devices they use to connect to the business network.

## Website Audits

- [ ] Make sure your website is updated **at least monthly** with the latest patches.
- [ ] Do a **yearly security audit** on your site.
- [ ] If your site is compromised, be ready with a **business continuity plan**.

## HR People

- [ ] The employee termination process must include the deletion of all employee logins when they leave the company; passwords they have used or shared must be changed (including those which allow for physical access or the setting of alarms).
- [ ] Train employees once a year on the dangers of cybersecurity, teach them why they are targets and how to be safer at home so they don't bring malware to work. Have them sign an understanding these rules, to take them seriously.
- [ ] Run threat simulations, and get any employees who fail additional training.

## IT

- [ ] Create a corporate password/pass phrase standard that all employees must adhere too.
- [ ] Add multi-factor authentication when possible.
- [ ] Back systems up continuously OFF THE NETWORK (ransomware will encrypt on-network backups) and test backups at least once a quarter.
- [ ] Ensure a disaster recovery/business continuity plan is in place and test it.
- [ ] Have a formal patch management system (ideally automated) where patches are received, prioritized and implemented.
- [ ] Ensure that default (factory set) passwords are changed on all hardware and software.
- [ ] All hardware should be installed with licensed (not free versions!) anti-virus and the anti-virus should be operational at all times.
- [ ] Conduct regular (automated) vulnerability scans of the network.
- [ ] Some level of penetration testing should be done at least annually.
- [ ] Change all default passwords on iOT enabled devices.

## Leadership

- [ ] Get Cyber Security Insurance (company)
- [ ] Create internal process around wire and payroll procedure, audit and update on a quarterly basis

*Note: A realistic goal is compliance with as many of these as possible, with efforts to close gaps on the rest – it is impossible to eliminate all cybersecurity risk.*


Special thanks to Arctic Wolf whose 24×7 Concierge Security™ Teams work around the clock to monitor, detect, and respond to cyberattacks before they have the chance to impact your business, for providing much of the wisdom in this document.