Below you will find the following sample policies:

- Antivirus and Malware Prevention Policy and Procedures (Template)
- Employee Personal Device Use Terms and Conditions (Template)

***Log in to eRisk Hub® for more and to download customizable word versions of the templates.**

The following is a template designed to assist in the policy development governing the protection of company computer systems and assets. As with all templates, this document provides a basic framework for the broad topics for consideration. Footnotes provide prompts for other general considerations and points for discussion. Each organization has unique risks and considerations that necessarily require customization. For more information, contact Ron Raether or Scot Ganow at (937) 227-3733 or rraether@ficlaw.com and sganow@ficlaw.com.

Antivirus and Malware Prevention Policy and Procedures (Template)

Purpose

The purpose of this policy is to set the minimum guidelines necessary to make sure that the confidentiality, integrity, and availability of data on the COMPANY Network are protected from hostile code such as malware, viruses, and worms. To do this, we deploy antivirus and malware prevention software on all systems of the COMPANY network as a mandatory standard.

Applicability

This policy applies to all computing environments, networks and computer systems owned, contracted, leased, or operated by COMPANY. It may also apply to personally-owned or third party computers transmitting our sensitive data electronically or connecting directly to the COMPANY Network, including any websites operated by us.

This policy applies to all users, including administrative consultants, employees, contractors, administrators, and third parties.

Policy

I. The willful introduction of a computer virus, malware, and disruptive/destructive code to the COMPANY Network is prohibited.

II. Information Technology is responsible for deploying and maintaining approved antivirus/malware prevention software to all systems it supports/ administers and providing timely updates for all components of the software on:

A. Any externally facing servers or gateways

B. Proxy servers

C. Application servers such as mail servers and/or mail gateways, FTP servers, web servers, audio/video servers

D. Data management servers such as back-up servers and database servers

E. COMPANY deployed desktops, laptops, and tablets

F. When technically feasible, cell phones, smart phones and PDAs (Please refer to the [INSERT APPLICABLE POLICIES][1])

G. For non-COMPANY deployed laptops or mobile devices, Information Technology should ensure that both up-to-date antivirus/malware prevention software and a personal firewall are deployed on the connecting device prior to granting permission to connect to the COMPANY Network.

III. Users are not to make any changes to their system that will disable or remove our approved antivirus and malware prevention software or otherwise prevent the software from performing its intended purpose.

IV. Users are not to open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. All unexpected content received from a trusted source should be verified with that source prior to opening.

V. Computer systems that are unable to run antivirus and malware prevention software must be restricted to an isolated network with sufficient network-level protections deployed to prevent viruses/malware from spreading into any other areas of our network (e.g. running antivirus technology at its "gateway" to the COMPANY Network).

VI. Antivirus/malware prevention updates will be installed and scheduled to run at regular intervals or upon electronic notification of a new security update, patch, vulnerability, or threat. Wherever possible, our computing resources should be set to auto-apply/update security patches on a regular basis.

VII. Antivirus and malware prevention scanning should be programmed to run/initiate upon startup and/or reboot of PCs/servers/other computing devices.

[1] As with all policies, this policy should compliment other company policies and not undermine other initiatives.

VIII. For PCs/servers/computing devices that are not normally rebooted, antivirus and malware scanning should be "always on" when technically feasible. If not possible, the Information Technology Department ("Information Technology")[2] should ensure that antivirus and malware remediation is accomplished for the protection of our electronic assets.

IX. Information Technology is responsible for receiving and acting upon alerts (via automated alert, email, news, etc.) promptly to ensure minimal exposure and security risk to the confidentiality, integrity, and availability of our electronic assets.

X. Critical security patches should be deployed by Information Technology a maximum of 48 hours after released by the operating system software or application vendor, unless there is reason to believe the patch might negatively impact a business-related activity or application.

XI. After appropriate testing, updates without issue will be made available to all PCs/servers/computing devices, as well as remote employees.

XII. Information Technology will run malware prevention software scans routinely (at a minimum weekly).

XIII. Information Technology will run antivirus and malware prevention software immediately after the installation of any new software, not normally supported by Information Technology.

XIV. Suspicious content (files or macros attached to email) should be quarantined for review or permanently deleted immediately.

XV. All downloads should be scanned with an updated COMPANY standard antivirus/malware prevention scanner immediately (automatically, if possible).

XVI. Computing systems will be rebooted as required to ensure virus definitions (as well as operating system updates) are updated and that the antivirus software can run to check for viruses.

XVII. Information Technology default settings should be set up so that antivirus software runs upon startup or reboot.

Compliance

Violations of this policy may lead to suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. In the case of a third party, there may be contractual obligations for encryption that the third party is responsible for implementing. Violations of those provisions may result in cancellation of any related privileges

[2] Likewise, coordination should take place with applicable departments to safeguard against conflicting procedures and policies.

or termination of the contract. We reserve the right to advise appropriate authorities of any violation of law.

Accountability

Information Technology is responsible for ensuring that Antivirus and Malware Prevention Policy and Procedures are followed.

Third parties/vendors are responsible for ensuring their use and access to COMPANY and our computing resources, whether on their own information assets or on our assets meets our security protections and safeguards and that the assets are used appropriately.

Internal Audit is responsible for ensuring compliance with the Antivirus and Malware Prevention Policy and Procedures and the controls created to safeguard the COMPANY Network.

Exceptions

The following types of network-enabled devices are approved exceptions by Information Security to this policy:

Device	Approver ID	Date	Last Reviewed
Type of device	Employee ID	Date	Last date

FARUKI IRELAND & COX P.L.L.
ATTORNEYS AT LAW
TRUSTED WISDOM. EXTRAORDINARY RESULTS.

The following is a template designed to assist in the policy development governing the protection of company computer systems and assets. As with all templates, this document provides a basic framework for the broad topics for consideration. Footnotes provide prompts for other general considerations and points for discussion. Each organization has unique risks and considerations that necessarily require customization. For more information, contact Ron Raether or Scot Ganow at (937) 227-3733 or rraether@ficlaw.com and sganow@ficlaw.com.

EMPLOYEE PERSONAL DEVICE USE TERMS AND CONDITIONS (TEMPLATE)

[COMPANY NAME] ("Company") provides its employees ("Associates") who acknowledge and agree to the terms and conditions below, the opportunity to use their own computers, smart phones, tablets, and other devices for business purposes to access and use Email and other authorized Company systems and information ("Company Data"). Access and use is subject to the following terms and conditions ("Terms and Conditions").

DEVICE REQUIREMENTS

1. "Personal Device" means a computer, smart phone, tablet, or other device that is authorized to access Company Data or is used to backup any such device and is owned by Associate and acquired voluntarily, without payment by Company and without any expectation of reimbursement for any costs related to the purchase, activation, operational/connectivity charges, service or repairs, or other costs that may be incurred related to the device or its use.

2. The Minimum Security Requirements[1] for using a Personal Device are listed below, but may be subject to change:

[1] Company may have additional security requirements, if operating in a regulated industry (i.e. healthcare) or an industry with its own self-regulatory requirements (i.e. PCI)

a. Password-protected[2] access;

b. A password/pin code must be entered on any Personal Device after fifteen (15) minutes of inactivity;

c. The Associate must maintain the original Personal Device operating system and keep the Personal Device current with security patches and updates, as released by the Personal Device manufacturer. The Associate will not "Jail Break" the Personal Device (installing software that allows the user to bypass standard built-in security features and controls) or otherwise modify the safeguards installed on the Personal Device by the manufacturer; and

d. The Personal Device must be encrypted and any resulting back-ups must also be encrypted[3].

3. If a Personal Device becomes non-compliant with any of the Minimum Security Requirements, it must be remedied within a reasonable period of time, or the Personal Device will be blocked from access to Company Data and the Personal Device may be remotely wiped (which will return it to factory default settings and may result in the deletion of personal information maintained on the Personal Device).

ASSOCIATE RESPONSIBILITIES AND CONDITIONS

1. Do not allow third parties to access or use any Company Data on or through your Personal Device.

2. Use of a Personal Device to access Company Data must comply with the Terms and Conditions and with the Company's [INSERT APPLICABLE COMPANY POLICIES], along with all federal, state, and other applicable laws.

3. Company Data must only be stored on a Personal Device as necessary, and storage of any Company Data must be kept to a minimum.

4. In order to participate under these Terms and Conditions, Associates must have permission from their manager. For non-exempt Associates accessing Company Data via a Personal Device outside of their scheduled work period, the access may constitute working time and manager approval must be sought prior to incurring any overtime hours[4].

5. In the event a Personal Device is lost, misplaced, or stolen, you must notify your manager or Information Technology Manager as soon as practical after you notice the device is missing. The Company may take appropriate actions, at its discretion, to safeguard

[2] Depending on the nature of the information or any regulatory restrictions, strong passwords may be required.
[3] Certain industries might have technical or regulatory requirements for such encryption.
[4] Consult counsel on legal questions regarding labor requirements for overtime-related matters.

Company Data, including remote wiping the device (which will return it to factory default settings and may result in the deletion of your personal information maintained on the device).

6. In the event a Personal Device is transferred to someone else for any reason, including a warranty replacement or for servicing by any person other than the Company's Information Technology Department, discarded, deactivated, or its use is otherwise discontinued, notification must be provided to the Information Technology Manager and any and all Company Data must be immediately and permanently deleted from the Personal Device before such transfer.

7. When Associates terminate their employment with the Company, Associates must, prior to their final working day with the Company, submit their Personal Device (and any applicable passwords, if required) to the Company in order to remove any and all Company Data and delete Company Data from any backup systems maintained by the Associate. The Company may take appropriate actions, at its discretion, to safeguard Company Data, including remote wiping the device (which will return it to factory default settings and may result in the deletion of your personal information maintained on the device) or seeking judicial intervention to compel submission of the Personal Device to inspection by the Company.

8. The Company's Information Technology Department will not provide any technical or services support for your personal applications or personal data on your Personal Device.

9. At the request of the Company's Human Resources or Information Technology Department, Associates must immediately surrender physical possession of their Personal Device (and any applicable passwords) to the Company.

10. Associates do not have a right of privacy nor should they expect privacy while using a Personal Device to access Company Data[5]. Any Personal Device is at all times subject to the Company's right to access the Personal Device, with or without notice, to monitor, investigate, review, delete, collect data, remote wipe data, and/or remotely disable the Personal Device at any time and for any reason. This may include the ability to view applications on the device and the ability to identify the location of the device through location-based services. The Company will not be liable for the loss of any personal data arising from such actions. The Company may also, at any time and without notice to you, collect information from a Personal Device for litigation or law enforcement purposes. By accepting this policy, Associates consent to disclosing and monitoring of Personal Device usage, including the contents of any files or information maintained or passed through that Personal Device.

[5] This area presents a great opportunity to proactively discuss the roll out and communication of the policy, to include employee expectations and what the company can/should do when it comes to information access. Experience counts here.

11. Unless permitted to do so by their Supervisor, Associates may not download, store, or transfer confidential or sensitive business data to their Personal Device. Confidential or sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual, outcome of a charge/complaint/case, the Company or third parties' proprietary information, or the Company's financial operations.

12. Upon direction by the Company, Associates agree to delete any sensitive business files that may be inadvertently downloaded and stored on the Personal Device through the process of viewing e-mail attachments.

13. In order to access Company Data on a Personal Device, Associates may be required to download and install specific applications or software. The Company shall not be liable or responsible for any viruses or any damages, loss of data, or any other costs or expenses incurred by Associates arising from such downloads or installation.

14. Associates shall indemnify and hold the Company harmless from and against any and all claims, damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to or resulting from any non-compliance with the Terms and Conditions. The Company is not responsible for any damages, loss of personal data or content, or any other costs or expenses incurred by Associates relating to the Personal Device.

USER ACKNOWLEDGMENT AND AGREEMENT

It is the Company's right to restrict or rescind computer privileges, or take other administrative or legal action due to failure to comply with the above Terms and Conditions. Violation of these rules may be grounds for disciplinary action, up to and including removal.

I acknowledge, understand, and will comply with this policy and rules of behavior, as applicable to my use of a Personal Device. I understand that addition of Company-provided third party software may decrease the available memory or storage on my personal device and that the Company is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third party software or use of the device in this program. I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by the Company's Information Technology Department. I understand that business use of a Personal Device may result in increases to my personal monthly service plan costs. I further understand that Company reimbursement of any business-related data/voice plan usage of my Personal Device is not provided.

Should I later decide to discontinue my use of a Personal Device, I will allow the Company to remove and disable any Company-provided third party software and services, and Company Data from my Personal Device.

Associate Name: _____

Associate Signature: _____

Date: _____

768559.1