Eagle Family Foods Group LLC and its Subsidiaries

# Mobile & Computing Resources Policy

Revised 4/2017

Company-provided Desktops, Laptops, Hardware, Software & Accessories

Workstations - Generally, a laptop computer will be provided to all office employees except for some plant locations. Office employees with desktop computers will be provided with a laptop during their next scheduled computer upgrade. Desktop computers remain available by request.

Unique Requirements - The Company's standard computer consists of hardware and software tools that meet most business needs. Unique business requirements may require the need for special software/hardware, which can be requested through the local Help Desk or Director of IT. Information Technology will purchase and test the special software and then install. Special hardware and software must be approved by your supervisor. Personally owned software is not to be installed on Company computers.

Printers - Centrally located network printers are provided in all office locations. The Company encourages the use of network printers, as they are more cost effective than personal printers. Circumstances that may justify a personal printer include frequent need for printing confidential data and/or a workspace that is not close to a network printer.

Working Remotely. - Sales/heavy remote users can also request a mobile air card (MiFi $50/month) with manager approval and notification to the Director of IT. Loaner MiFi's are available. Remote access to company internal systems may require a Secure ID, which can be requested through the local Help Desk or Director of IT. Personal home wireless networks should always be secured. Guidance will be available from the Help Desk.

Acceptable Use - Information Technology will monitor all mobile and computing resources that access the Company Network, Company email and applications, or store Company data. However, it is every employee's duty and responsibility to protect the confidentiality and security of Company information and systems.

The guidelines below are provided as a resource and are not all inclusive. If you have questions, please contact your immediate supervisor.

- The company reserves the right to monitor and/or log all computer activity of users without notice, including all email and internet connections. As property of the Company, the content of all such records, including email, is subject to inspection at any time by Company personnel.

- The company owns the rights to all Company information assets (data and files) on any Company connected assets or systems. Employees do not have, and should not expect to have any right to privacy concerning what is contained in or passes through the Company's computing assets and systems, including but not limited to email, instant messaging, enterprise applications, voice mail, telephones, and Internet usage. The Company reserves the right to access and disclose files, documents, or communications stored on its property or on any device connected to Company systems to assure proper use and to prevent security incidents.

- Acceptable personal use includes occasional access to the Internet for personal email, information, and social networking.

- Personal use of Company computer systems is permitted on an occasional basis if such use:

    - Is not in pursuit of any outside business interests, gambling or political causes.
    - Does not interfere with or detract from the employee's fulfillment of his or her duties and obligations to the Company.
    - Does not impact the response times of the Company's computing assets and computer systems, or negatively impact third party computing assets (e.g., music and video streaming, sharing, or downloading).
    - Does not involve the copying or transmission of any material in violation of the privacy, copyright, or property rights of others.

- Applications, such as iTunes and Blackberry Manager, are not permitted to be installed on a Company asset without approval from your supervisor and the Director of IT.
- Company information will not be backed up to Internet back up sites such as iCloud or MobileMe.
- The Company is not responsible to back up personal information.
- Personally licensed software is not to be installed on company assets.
- Employees may not use Company assets and systems for any communications, incoming or outgoing, of any illegal, offensive, discriminatory, harassing, threatening, or obscene nature.
- The employee must comply with all laws (including, but not limited to, safety/vehicular, copyright, licensing, and intellectual property).
- The employees will not disable, uninstall, or otherwise circumvent any Company or device manufacturer's inherent security settings. The employee is also responsible to keep all systems, applications and software current and updated, as needed.
- Employees are responsible for all system activity associated with their Company provided User ID. Once Company system access is implemented on a device, it is no longer appropriate to allow unmonitored access to the device.
- Employees must immediately report any lost computers, mobile devices, or air cards, any suspicious activity or misuse of Company computing assets and systems to his/her manager, the local Help Desk, the Company's HR department, or the Director of IT.

## Mobile Devices

Mobile devices represent a significant risk to information/data security as, if the appropriate security applications and procedures are not followed, they can be a conduit for unauthorized access to the Company's IT and data infrastructure leading to data leakage and system issues.

The Company must protect its information assets to safeguard its customers, intellectual property, and reputation. As such, the Company has adopted the following requirements:

Technical Requirements

(1) Devices must use the following operating systems: Android and iOS;
(2) Devices must store all user-saved passwords in an encrypted password store, example Password Safe;
(3) Devices must be configured with a secure password that complies with the Company's password policy. That password must not be the same as any other password or credentials used within the Company by the user;

User Requirements

(1) Users must only load data essential to their role onto their mobile devices;
(2) Users must report all lost or stolen devices as to Company's IT Department immediately;
(3) If a user suspects that any unauthorized access to Company data has occurred, the user must report that suspicion to the Company's IT Department immediately;
(4) Users must not load pirated software or illegal content onto their devices;
(5) Applications must only be installed from official platform-owner approved sources (iTunes or Google Play). If a user is unsure if an application is from an approved source, contact the Company's IT Department;
(6) Devices must be kept up to date with manufacturer or network provided patches;
(7) Devices must be encrypted in line with the Company's standards;
(8) User must ensure that Company data is sent only through the Company's email system. If a user knows or suspects that Company data has been sent from, through, or to a personal email account, the user must immediately notify the Company's IT Department; and
(9) Devices must not be "jailbroken" or have any software or application installed which is designed to gain functionality not intended to be exposed to the user.

Device Reimbursement - All mobile devices should be employee-owned.

Mobile Device Reimbursement - The plan must be in the employee's name and is her or her responsibility. Plans should be selected based on the following usage patterns. Most plans now provide unlimited voice/text and focus on data usage (e.g., 8GB/month). You can temporarily increase your data plan during high travel months to control cost or contact IT for a hotspot.

- All salaried employees will receive a monthly phone stipend of $75 (subject to position and company approval). You will be provided this stipend in the first pay period of each month.

- All salaried Sales employees will receive a monthly phone stipend of $125. You will be provided this stipend in the first pay period of each month.