ECOSSENTIAL FOODS CORPORATION

IT POLICY AND PROCEDURE

IT TEAM

ECOSSENTIAL FOODS CORPORATION

Updated 2023

EFC - IT Policy and Procedure Manual

Table of Contents

Table of contents 1
Introduction 2
Technology Hardware Purchasing Policy 3
Purpose of the Policy.. 3
Procedures.. 3-5
Policy for Getting Software.. 6
Purpose of the Policy.. 6
Procedures.. 6-7
Policy for Use of Software 8
Purpose of the Policy.. 8
Procedures.. 8
Bring Your Own Device Policy.. 9
Purpose of the Policy.. 9
Procedures.. 9
Information Technology Security Policy 10
Purpose of the Policy.. 10
Procedures.. 10-11
Information Technology Administration Policy.. 12
Purpose of the Policy.. 12
Procedures.. 12
IT Service Agreements Policy.. 13
Purpose of the Policy.. 13
Procedures.. 13-14
Emergency Management of Information Technology.. 15
Purpose of the Policy.. 15
Procedures.. 15

Data Privacy Act

Purpose of the Policy.. 16
Procedures.. 16-17

Asset Management

Inventory Control 18
Equipment/Device Egress 19-20
Asset Disposal 21
Laptop Issuance/Turn-over 22-23
Bidding Process 24
CRF 25

Cyber Security

Virus/Malware Detection/Removal 26
Spam handling/Domain Reputation 27

Introduction

EFC IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT personnel within the EFC organization which must be followed by all Employee.

EFC will use these guidelines to administer these policies, with the correct procedure to follow. IT team will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

Technology Hardware Purchasing Policy

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the company to ensure that all hardware technology of EFC is appropriate. The objective of this policy is to ensure that all purchase request is within the approved budget for the year, requested by the requesting Department and checked by IT personnel or otherwise approved by the Management in case it is not budgeted.

Procedures Purchase of Hardware Guidance:

The purchase of all desktops, servers, portable computers, computer peripherals, cctv components and other devices must adhere to this policy. Request should be initiated by the requesting Department with the approval/signature of the department head. IT personnel may prepare the PRS and list the specification of the hardware and put remarks if within the budget or not and sign the PRS before forwarding to the Signatory (currently HR director). The signed PRS will be then forwarded to the Purchasing Officer for processing.

The desktop computer system bundle must include:

Casing w/ psu/fan
Motherboard, CPU, RAM, HDD/SSD
Monitor, Keyboard, Mouse, UPS

With a minimum specification:

Core i3, 8GB ram, 1TB HDD/500GB SSD.

Other peripherals may include but not limited to:

Videocard, soundcard, additional HDD/SSD, additional monitor

The laptop computer system bundle must include:

Laptop unit, Charger, Bag

With a minimum specification:

Corei3, 500gb SSD, 8GB RAM

Other peripherals that can be requested with approval:

Mouse, Flashdrives/External Drive

Purchasing server systems:

On-premise server systems can only be requested by IT department considering it is budgeted or urgently needed with the approval of the higher management.

The server system bundle requirements may consist of the ff but not limited to:

Motherboard, CPU's, RAM's
Network fabric
Storage – harddrives/SAN
PSU – built in/redundant
Videocard/Monitor
Server chassis

Network and Security Components:

List of network devices and security appliance that can be requested are as follows but not limited to:

Firewall
Router/Switches
Access point/ Wifi connection
Network cabinets
Server UPS
CCTV

Warranty & Life Span

Usual warranty of purchased IT hardware are as follows:

Hardware	default warranty	w/extended warranty
Desktop	1 year	
Laptop	1 year	3years
Peripheral	1 year	
Server	1 year	Renewed Annually

If IT hardware became defective on its warranty period, IT personnel should report and schedule a warranty claim to the provider/supplier. If the warranty period already expired, IT should assess if it will be subject for repair or subject to replacement.

Expected Life Span of IT Hardware:

Hardware	Life Span	Replacement period
Desktop	4 -5 years	6 years
Laptop	3-4 years	5 years
Peripheral	1-3 years	
Server	5 years	7 years
Network Devices	5 years	7 years

If the IT hardware falls on the life span period, IT will assess the hardware if its still working as intended/presentable or needs to be replace.

IT will consider the replacement of the hardware devices if it falls on the replacement period or parts/components is already obsolete in the market.

Policy for Getting Software

Purpose of the Policy

This policy provides guidelines for the purchase of software for the EFC organization to ensure that all software used is legal, value for money and where applicable integrates with other technology for the company. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures of Purchasing Software/Software Licenses:

Request should be initiated by the requesting Department with the approval/signature of the department head. IT personnel may prepare the PRS and list the specification of the software and put remarks if within the budget or not and sign the PRS before forwarding to the Signatory (currently HR director). The signed PRS will be then forwarded to the Purchasing Officer for processing.

For bundled software's, latest issue/version should be considered and compatibility must be prioritized. IT personnel must ensure that the software products are genuine and not pirated/tampered to assure that the company complies to EULA or GPL.

Sample of software licenses bundled on hardware as package:

Windows Operating System
Microsoft Offices
Window Server Edition

Sample of software licenses separately purchased as per request:

MS Visio
MS Access
Adobe Photoshop

As a general rule, all software request that is not included on IT's default list during configuration is subject for approval of Department head and Management.

IT default software list on Desktop/Laptop installation:

- Operating System such as Windows/iOS
- Office App such as MS office
- Web Browser such as Google Chrome
- PDF reader such as Adobe Reader
- Remote Session Tool such as Teamviewer and Anydesk
- Anti-Virus such as Sophos
- Instant Messaging App such as Viber
- Video Conferencing App such as Zoom

IT Department can prohibit any purchase/installation request of software's that did not meet the qualification as follows:

- Will be use for work related or job function
- Legal or not against the law
- No virus/malware detection
- Does not contain any malicious script
- Not pirated/ Counterfeit

Policy for Use of Software

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the EFC organization to ensure that all software use is appropriate. Under this policy, the use of all installed software/application is strictly for the EFC day to day operations or work-related activities only.

Procedures

Only software obtained in accordance with the getting software policy is to be installed on the company computers. Modification and tampering of installed software or application is strictly prohibited. Installation and use of application for the purpose or related but not limited to hacking, games, drugs, cyber criminal activities, pornography, unlawful act is strictly prohibited and will be subject to penalty and punishment by the company.

Bring Your Own Device Policy

Purpose of the Policy

This policy provides guidelines for the use of personally owned laptops, smart phones, tablets and other devices for work purposes. All staff/guest who use or access EFC's network connections such as WiFi or LAN's are bound by the conditions of this Policy.

Procedures

Any BYOD/Guest devices must be check by IT Dept before connecting to EFC's network resources. IT personnel can reject or prohibit the request of employee/guest to connect on EFC's network for the following reasons:

No updated anti-virus is installed on the device
Unknown or malicious software is installed on the device
Not work-related purpose
Device shows security threat

By default, mobile devices are not allowed to connect on EFC network unless it is approved by the management and registered to the system. IT personnel can reject/blocked any device which exhibit malicious traffic or bandwidth consumption and will be subject to investigation with the use of networking tools.

This policy also indicates that any employee or guest who connects their BYOD to EFC's network agrees not to download or transfer institution or personal sensitive information to the device as part of the DPA compliance.

Information Technology Security Policy

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the EFC organization to ensure integrity, confidentiality and availability of data and assets.

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation, door locks/biometrics authentication, CCTV captured angle. It will be the responsibility of IT Officer to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the IT officer immediately. All security and safety of all portable technology, laptop, mobile phones, other devices will be the responsibility of the employee who has been issued with the accountability for such device. Each employee is required to use any form of security like locks and password to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, management will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage

All devices such as Desktop/Laptop when kept at the office desk, is to be secured by office door lock provided by the building admin.

Information Security

All data and information related to job description of the employee and personal information controller/processor is to be kept confidential, stored in a protected folder or drives and is to be backed-up to a secured network drive or cloud storage. It is the responsibility of the IT Officer to ensure that data back-ups are conducted and the backed-up data is kept on on-premise file storage or cloud storage. All technology that has internet access must have anti-virus software installed. It is the responsibility of IT Analyst to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution. All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. Any employee breaching this will be penalized and will face criminal liability under R.A. 10173 or DPA of 2012.

Technology Access

Every employee will be issued with his/her own username & password to access the EFC technology such as Desktop/Laptop & email login. Each password needs to be a combination of Alpha numeric with a minimum of 8 characters long and is not to be shared with any employee within the company. IT personnel is responsible for the issuing of the username and initial password for all employees. Where an employee forgets the password then the IT Analyst is authorized to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password. Employees are only authorized to use EFC computers for work-related use.

It is the responsibility of IT Officer to keep all procedures for this policy up to date.

Information Technology Administration Policy

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the EFC organization.

Procedures

All software installed and the license information must be recorded on the IT logs and Netsuite. It is the responsibility of IT Analyst and System Admins to ensure that this record is maintained.

IT Officer is responsible for the maintenance and management of all service agreements for the EFC technology. Any service requirements must first be approved by HR Director.

IT Analyst is responsible for maintaining adequate technology spare parts and other requirements including Desktop/Laptop peripherals, Monitors, keyboards, UPS, power Supply, etc.

Admin controls & authority are in place such as the IT officer is the one with admin login while IT Analyst have their monitoring login and the HR director will be having her Super Admin login.

IT Service Agreements Policy

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the EFC organization.

Procedures

The following IT service agreements can be entered into on behalf of the EFC organization:

- Provision of Security Devices and software
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of Applicaiton software
- Provision of Internet Services
- Provision of CCTV systems and camera

All IT service agreements must be reviewed by IT Officer and HR Director before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by HR Director/Management.

All IT service agreements, obligations and renewals must be recorded (hard copies should be kept on folders kept in a secured locker or drawer).

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorized by HR Director.

Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, IT Officer and HR Director will review it before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by HR Director/Management.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to the IT Officer who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the EFC organization.

Procedures

IT Hardware Failure

Where there is failure of any of the IT hardware, this must be referred to IT officer immediately. It is the responsibility of IT Officer to provide Emergency backup Plan in the event of IT hardware failure. It is the responsibility of IT Officer to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimize disruption to EFC operations.

Virus or other security breach

In the event that the EFC information technology is compromised by software virus/malware or phishing, such breaches are to be reported to IT team immediately. The IT Officer is responsible for ensuring that any security breach is dealt with within 1hr to 1 day depends on the severity of the detection to minimize disruption to EFC operations.

Data Privacy Act

Purpose

To inform the EFC Community about the DPA in order to avoid violations. To teach EFC personnel to identify personal information processed and to know the proper treatment of the same.

Procedure

Orientation

Old and New employee’s will have their orientation regarding DPA. Data privacy coverage will be discussed and will be focusing on personal information and sensitive personal information. Any information from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information.

Consent of the data subject or employee will be requested on a formal written method indicating the purpose of the company to process any information or data given by the data subject.

Security Obligation

EFC employee must implement measures against:

- Accidental or unlawful destruction, alteration and isclosure.
- Unlawful processing.
- Natural dangers.
- Human dangers.
- Unlawful access.
- Fraudulent misuse.
- Unlawful distruction, altration and contamination

In case of Breach

Concealment of breach is a crime and therefore we should report the breach within 72 hours from knowledge of breach or else criminal liability can be impose with penalties amounting to 500,000 to 1,000,000 pesos and imprisonment from 1 year up to 7 years.

Breach reporting

Any individual who discover data breach within the company should report to the Data Privacy officer. The DPO then report to the security incident response team to ensure timely action will take place such as mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach. The DPO should then report to the NPC if the these are all present:

- There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;
- The data is reasonably believed to have been acquired by an unauthorized person; and
- Either the personal information controller or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

The following information must be included in any Data Breach notification:

- Nature of the Breach
- Personal Data Involved
- Remedial Measures
- Name and contact details

Inventory Controls (Laptop/Desktop/ Peripherals)

Purpose of the Policy

The purpose of the inventory control policy for laptops, desktops, and other peripherals is to establish guidelines and procedures for the management, tracking, and control of EFC hardware assets. The policy aims to ensure that all equipment is accounted for, in good working condition, and properly secured to prevent loss, theft, or unauthorized access.

Procedures

Inventory control procedures for laptops, desktops, and peripherals generally involve the following steps:

1. Conducting an initial inventory: This involves creating a detailed list of all the laptops, desktops, and peripherals. This is done by manually listing each brand-new or old laptop details on the IT inventory.

2. Asset tagging: For brand-new laptops, desktops, or other peripherals, a unique identifier, such as an asset tag or serial number, should be assigned. This will make it easier to track and locate items. Asset tags are provided by the Purchasing Department.

3. Establishing storage locations: Laptops, desktops, and peripherals will be stored in the EFC server room when they are not in use.
4. Implementing a check-in/check-out system: IT personnel will update the status of a laptop once it is issued or returned.

5. Conducting regular audits: IT personnel will review the inventory to ensure all the laptops, desktops, and other peripherals are accounted for. This can be done by physical counting.

Equipment/Device Outgress (gatepass)

Purpose of the Policy

The purpose of a policy for IT equipment and device outflow (gateway) is to establish guidelines and procedures for the proper management and control of the movement of IT equipment and devices within EFC. This policy ensures that IT equipment and devices are tracked, controlled, and properly secured when they are moved outside the EFC premises.

Procedures

IT personnel will make a gate pass form for every asset that will be moved outside and that needs to be signed by an available approver. After it is approved, it is needed to be signed by the guard in charge and by the receiver of the asset.

PRS (Purchase Requisition Slip)

Purpose of the Policy

The purpose of a policy for IT purchase requisition slips is to establish guidelines and procedures for the acquisition of IT assets and services. This policy typically outlines the process for submitting a request for IT purchases, the criteria for evaluating and approving such requests, and the responsibilities of various stakeholders involved in the purchasing process.

The policy for IT purchase requisition slips helps ensure that the organization procures IT assets and services that meet its needs and are in line with its budgetary constraints. It also helps prevent unauthorized or unnecessary purchases, ensures that purchases are made from reputable vendors, and promotes transparency and accountability in the procurement process.

Procedures

Requests for IT equipment or services must be initiated by the requesting department, individual, or IT personnel by completing an IT Purchase Request Form. The form should include details such as the type of equipment or specification required, quantity, budget allocation, and other relevant information.

Once the PRS has been reviewed and approved by the IT department head, the procurement team will generate a purchase order and submit it to the vendor. The purchase order should include details such as the vendor's name, product or service details, quantity, price, and delivery date.

Upon receipt of IT equipment or services, the IT personnel must inspect the items to ensure that they match the order and meet the quality standards.

The procurement team should process payment to the vendor once the equipment or service has been received and inspected. The procurement team also needs to issue an asset tag.

All documents related to the IT Purchase Requisition Slip, purchase order, and receipt of the IT equipment or service should be properly documented and maintained for future reference.

Asset Disposal Process

Purpose of the Policy

The purpose of a policy for the asset disposal process is to provide a standardized and controlled process for disposing of outdated, unused, or defective assets in the company. This policy outlines the criteria and process for selling or disposing of EFC's assets, ensuring that the IT department obtains the best value for its assets and that sensitive information is protected.

Procedures

After identifying which asset is needed to be disposed (such as age, condition) the IT personnel will inform the finance department and prepare an asset disposal form signed by the authorized approver.

Disposal can be categorized into two types: disposal through sale and disposal through write-off.

Disposal through sale is the act of disposing by selling the asset. IT personnel will find bidders and make a proposal to the Finance Department. Once approved, IT personnel will create an asset disposal form and gate pass for the assets.

Disposal through write-off is the act of disposing of an asset without any value. This is usually for assets such as a mouse, keyboard, laptop battery, UPS battery, etc.

Laptop issuance and turnover policy

Purpose of the Policy

The purpose of a laptop issuance and turnover policy is to establish guidelines for the distribution and management of laptops within the EFC. The policy outlines the responsibilities of employees, IT staff, and other stakeholders involved in the issuance and turnover processes. It provides a framework for ensuring that laptops are used effectively, securely, and in compliance with IT policies and regulations.
Procedures.

Procedures
Laptop issuance:

Eligibility: Determine who is eligible to receive a laptop based on job responsibilities or if he or she is an employee replacement.

Request: Department managers may request a laptop via email. The request should include the employee's job responsibilities or the reason for the request (if it is a temporary or permanent issuance).

Approval: After the request is reviewed and approved by the appropriate manager, IT personnel will find a laptop for the request.

Configuration: The IT personnel configures the laptop with the appropriate software, security settings, and other requirements. For other laptops on other DCs, the IT personnel will remotely access the laptop.

Issuance: This is when the IT personnel will issue the laptop together with the accountability form, which is either a hard copy or sent via email and needs to be signed by the employee. As with other DCs, the FAO will be the one who issues the laptop with an accountability form and an asset transfer form.

Laptop Turn-over:

Notification: The employee who is leaving or whose laptop is no longer needed should notify their manager or IT personnel.

Data Removal: The IT personnel will remove all organization-related data and software from the laptop and may conduct a data wipe to ensure that all sensitive data is securely erased. This also includes disabling the company email of the resigned employee.

Asset Tracking: The IT personnel at the head office will update the IT inventory tracking to reflect the return of the laptop. For other DCs, the FAO will also update their laptop list monitoring, provided by the IT personnel.

Return: The employee returns the laptop to the IT personnel in the head office or to the FAO of each DC and signs a confirmation of return, the asset transfer form**.**

Bidding process

Purpose of the Policy

The purpose of a policy for the company bidding process is to provide a standardized and fair process for disposing of outdated or unused laptops in an organization. This policy outlines the criteria and process for selling or disposing of old laptops, ensuring that the company obtains the best value for its assets and that sensitive information is protected.

Procedures

The IT personnel specify the conditions under which laptops may be disposed of, such as age and condition.

After identifying which laptop should be disposed of for bidding, the IT personnel will need to provide a list of information about the laptops, such as the model, serial number, date acquired, and market value once it is confirmed to the finance department that it has fully depreciated. The IT personnel also needs to provide an asset disposal form with the details of the laptops, signed by the authorized approver (IT manager and finance department).

The IT personnel needs to prepare and setup the laptop and need to make sure that the laptop is formatted and all data is securely erased.

CRF (Check Request Forms)

Purpose of the Policy

The purpose of a policy for IT check request forms is to establish guidelines and procedures for the proper and efficient management of financial transactions related to IT purchases and expenses. This policy ensures that all IT expenses are properly authorized, documented, and recorded and that the funds are used in accordance with the IT budget and financial plan.

This policy also helps to ensure that IT purchases and expenses are properly tracked and managed, which can help optimize IT spending and minimize unnecessary assets or service purchases. By putting in place budgetary controls and approval limits, this policy ensures that IT spending is aligned with the IT annual budget.

Procedures

The IT personnel or requesting department should make a check request form, which includes the details such as the vendor's name, product or service details, amount of payment, and any other relevant information together with the sales invoice.

Once the Check Request Form has been approved, the finance department will process the payment to the vendor.

All documents related to the Check Request Form, including supporting documentation, invoices, and receipts, should be properly documented and maintained for future reference by the assigned IT personnel.

Process for Virus/Malware Detection/Removal

Purpose of the Policy

This policy provides guidelines to establish a standardized and effective approach for identifying, containing, and eliminating viruses and malware from computer systems and networks. The policy should outline the steps that must be taken by all personnel to detect and remove viruses and malware, as well as establish protocols for preventing future infections.

Procedures for Virus/Malware Removal

Every morning, IT personnel should check Sophos Central for possible detection. If there is a detected virus or malware, I.T. personnel should immediately contact the user for a remote session to initially check the system. Most of the time, Sophos will automatically clean up the virus or malware, but it is still our best practice to check the infected unit or units.

Process of the removal

1. Once there is an alert on the central Sophos dashboard, IT personnel will trigger the scan.
2. Investigate further if the alert is legitimate malware or a false detection.
3. If it is legit malware, IT personnel should disable the email and change the password to avoid spam on the user's email, then contact the employee for a remote session.
4. Check the device for any remaining malware files and delete them, then restart the manual scan in the Sophos app.
5. If the device is already secured, paste again the new email password and close the alert in the Sophos central dashboard.

For other urgent and high-risk issues, kindly send your email to Sophos Support with the following details:

Encountered issue:
Sample of a screenshot:

Then send your email to support@isolutions.com.ph and cc all IT personnel.

Spam handling and Domain Reputation

Purpose of the Policy

To Protect EFC organization from email spam attacks and maintain a positive domain reputation.
Ensure that all email communications sent from our organization are legitimate and to comply with all relevant laws and regulations.
Outline the steps that employees should take if they encounter spam emails or suspect that our organization's domain reputation has been compromised.

Procedure for spam handling and domain reputation

If an employee receives a suspicious email, they should notify the IT Team and forward the suspicious email.

Once the email is received by IT, they should check the sender and further investigate the email in the WHM.

If the suspicious email is accidentally clicked by the employee, the user should report it to IT for further checking, email will be temporarily be suspended, and the password must be changed. Check the procedure for virus/malware removal and investigate further to make sure that the employee devices are safe.