The Alaska Community Foundation

Information Technology (IT) Policies & Procedures

Table of Contents

1. INTRODUCTION

Purpose

The Alaska Community Foundation (the "Foundation") has developed the following policies and procedures for three primary reasons. First, they safeguard the Foundation business operations and information. Second, they safeguard staff productivity. Third, policies and procedures safeguard the IT assets, and ensure their cost effective long-term maintenance. These policies and procedures will continue to be expanded and revised as required.

Overview of the policy for computers, networks, and email

The Foundation provides staff with access to computers and computer network facilities, including electronic mail service, to conduct official Foundation business; and facilitate the flow of information both internally and externally.

The Foundation computers and network facilities should be used for the "The Alaska Community Foundation purposes" stated above. Commercial use of Foundation facilities is strictly prohibited at all times. All users of the Foundation's computer and computer network facilities must comply with applicable state and federal laws. The Foundation's computer and network users should be aware that email information that is stored and transmitted may not be secure and should not, therefore, be considered to be confidential. All email is the property of the Foundation.

Strategic Overview

The Foundation's formal IT Strategy is evolving over time. However, efforts within the Foundation's IT environment have been specifically designed to provide a sound infrastructure while controlling the environment to ensure that ongoing standardization and reliability are primary objectives.

Tactical Overview

The Foundation has engaged a third party provider of managed, outsourced IT services to provide its day-to-day services. The contract documents can be viewed at any time upon request.

Managed Service Provider (MSP)

Because the IT environment requires consistent care and feeding at the tactical (daily operating) level, the Foundation has contracted with **LMJ Consulting**.

The Foundation staff is encouraged to communicate emerging needs directly to the Operations Manager or staff IT Single Point of Contact (SPOC) who will indicate if appropriate for you to contact the MSP for assistance by either e-mailing **support@lmjconsulting.com** or calling **907-269-4324**.

2. DESKTOP SYSTEM (PC) POLICIES

Purpose

The purpose of desktop system (software and hardware) policies is to educate Foundation employees regarding the consistent, safe and legal use of organization-owned information

technology assets while simultaneously safeguarding employee productivity and critical Foundation business operations/assets.

Hardware and Peripherals

The hardware and peripherals provided are the property of the Foundation. All hardware and peripherals should remain where situated unless instructed by the MSP to do otherwise.

Hardware and Peripheral Problems

For hardware or peripheral problems, the operator refers to the operating manual. If the issue is not obvious, the user should try a regular restart. If the problem still cannot be corrected, the problem and its effect on the device(s) are noted, the user should contact the MSP directly and post a sign on the (desktop) PC or other item indicating it is not working and is not to be used. If a peripheral device does not work, the user should place a sign on the device noting that it is out of order and indicating whether or not the computer is useable without the device.

Software

The software provided is the property of the Foundation. All software should remain where it is unless instructed by the MSP to do otherwise. In general, downloading of organization-owned software is not permitted to privately owned computers or secondary storage in any form. Some exceptions may be made at the discretion of the President & CEO in certain instances such as with some Microsoft Office 365 licensing which can be downloaded on several devices.

Purchased Software

The user sends a memo requesting software to SPOC who reviews the request and, upon approval, will send the purchase request to the MSP who will issue a purchase requisition on behalf of the Foundation.

Software Licenses

The MSP maintains software licenses. MSP maintains MS Office install media and most other license keys on its internal documentation system.

Software Registration

All software registration will be handled, completed, and mailed by the MSP in the Foundation's name.

Backup Procedures

While not all data and software have the same value (although it is better to be safe if not sure), the following procedures are recommended:

New software backup procedures

New purchased software is backed up by the MSP in accordance with the software manufacturer's specifications.

Hard drive backup procedures

All users will save new documents and changes to existing documents on the network. All documents saved in the network are backed up nightly to the Foundation's on-site system and also to a cloud based backup system. Documents are never to be saved elsewhere (desktop, etc.) because they will not be backed up.

A backup copy of the hard drive software will be maintained by the MSP.

Software Problems

For software problems, the operator contacts the MSP. If the MSP's technician cannot resolve the problem, the MSP will escalate the issue internally. Before contacting the MSP for assistance, the operator will:

1. Note the details of what happened.
2. Note what corrective measures were tried.
3. Check in with the Operations Manager or SPOC.
4. If advised to do so contact the MSP using the phone number or email provided in section 1, Managed Service Provider of this document.

Personal Hardware and Software

No personal hardware or software (including screensavers and games) is allowed with the exception of mobile devices. All hardware, with the exception of mobile devices, and software of any kind, including in-house-developed programs, are the Foundation's sole property. This policy is enforced to reduce significant license and intellectual liability, problems with equipment, software failure, damage to data files, and the introduction of viruses. To restrict access to the Foundation's data and/or programs and prevent virus transmission, disks or tapes belonging to ACF are not to be used in personal home computers. USB drives (any USB drive, zip drives, thumb drives, external hard drives) shall not be used for file storage as they present virus and security risks. If a file must be transported, employees should use email to do so, unless the materials contain sensitive information.

For convenience, guests may use a USB drive in a conference room computer. Staff must login as a guest onto the computer and scan the USB drive with the current virus protection software prior to opening any files.

3. NETWORK MANAGEMENT POLICIES

Purpose

The purpose of network management policies is to educate Foundation employees regarding the consistent, safe and legal use of organization owned information technology assets while simultaneously safeguarding employee productivity and critical Foundation business operations / assets.

Overview

Networked PC systems and work group systems hardware configurations and support needs are more intricate. The network of computers depends on the system server. The network is unique; by itself it can shut down all computing in an enterprise—a single point of failure. For the Foundation, the network consists of a robust configuration, mitigating the risk associated with 'a single point of failure'. The Foundation's network and its performance are the responsibility of the MSP, a third party provider. No Foundation personnel are authorized to do work directly on the server unless authorized by the President & CEO. The President & CEO and the CFO may have terminal server access if and when determined necessary.

Disk to Disk Backup Procedure

Nightly backups are a critical business data recovery procedure (see Section 9). The combination of individual users properly utilizing the server's shared drive and the MSP's management of Disk To Disk backup is the single best method of protecting the Foundation's information assets. If executed consistently, under a worst-case scenario, the risk of loss to critical Foundation data or information assets will be limited to a single business day.

Procedure Steps:

1. MSP to verify and daily check backup logs on Disk to Disk Appliance.
2. Backups are replicated to the secured cloud storage servers nightly.
3. MSP documents backups daily (maintained in system logs)
4. Configure job for automatic completion.
5. Immediately notify contact Disk To Disk backup vendor immediately if there are problems with the backup routine.

4. 'What If I Need Help' POLICIES

Purpose

The purpose of 'What If I Need Help' policies is to educate the Foundation employees regarding the consistent documentation and escalation of all computer-related issues that threaten employee productivity or the Foundation information assets.

Overview

All network, hardware and software issues should be communicated to the SPOC for assistance. The SPOC will determine if the MSP or another software/hardware provider needs to be contacted. When communicating with the MSP or another software/hardware provider, please document (copy any error messages or dialogue boxes) and label issues as one of the following:

- Hardware
- Software
- Connectivity

Indicate either:

1. Work stoppage (no work around available and work cannot be accomplished).
2. Work around available. This will help assess the priority and the proper Service Level Agreement for response.
3. Contact the MSP using the phone number or email provided in section 1. Managed Service Provider (MSP) of this document. The SPOC can provide other contact information as necessary.

5. ELECTRONIC COMMUNICATION POLICY

Purpose

The Foundation maintains an electronic communication system to assist with the conduct of business within the organization. The electronic communication policy formalizes standards for how the organization connects to the outside world though the use of electronic communications – fax, e-mail, telephone, instant messaging, authorized mobile devices and the Internet. Electronic communications are valuable and costly corporate resources and must be used only for organization business. While electronic communication provides access to a wealth of valuable information and facilitates communication, it also opens the potential for others to access the organization's valuable proprietary information. Irresponsible use of electronic communications reduces their availability for critical business operations, compromises corporate security and network integrity, and leaves the organization open to potentially damaging litigation.

Scope

The electronic communication policy covers all types of connections to the outside world including through the Internet. The policy also covers all activities performed while using the Internet, including but not limited to browsing (viewing Web pages), using email, instant messaging, transferring files using FTP (file transfer protocol) and use of authorized mobile devices.

Policy Objectives

This policy provides guidelines ensuring the secure, proper, and reliable use of electronic communications. The Foundation's electronic communications policy are part of the new employee orientation process. Any new or existing employee signs an acknowledgment that he/she has received a copy of this policy and is responsible for its content.

Electronic Communications Guidelines:

Acceptable uses of organization internet access and electronic communications

The Foundation provides internet and electronic communication access for business usage. Every staff member has the responsibility to maintain and enhance the organization's public image and to use organization access to the internet and electronic communication in a manner that reflects well on the organization. The Foundation recognizes there will be

occasional personal use on lunch breaks and during nonworking hours (with the approval of management), but this shall not be excessive or unreasonable.

Unacceptable uses of organization internet access and electronic communications

The Foundation internet access and electronic communications may not be used for transmitting, retrieving, or storage of any communications that would violate the Foundation's policy including but not limited to that of a discriminatory or harassing nature or materials that are obscene or "X-rated." Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference shall be transmitted. No excessively abusive, profane, or offensive language is to be transmitted through the organization's email or Internet system.

Electronic media also may not be used for any purpose that is illegal, against organization policy, or contrary to the organization's best interests. Any non-Foundation commercial use and / or solicitation of non-organization business, or any use of the organization email or Internet for personal gain, should be disclosed in the Confidentiality and Conflict of Interest Policy and pre-approved by the President & CEO.

Communications

Each employee is responsible for the content of all text, audio, or images that he/she places or sends over the organization's email and Internet system. No email or other electronic communications may be sent hiding the identity of the sender or representing the sender as someone else or someone from another organization. All messages communicated on the organization's email and Internet system should contain the employee's name.

Any messages or information sent by an employee to another individual outside the organization via an electronic network (e.g., bulletin board, online service, or Internet) are statements that reflect on the organization. While some users include personal "disclaimers" in electronic messages, there is still a connection to the organization, and the statements may legally be tied to the organization. Therefore, the Foundation requires all communications sent by employees via the organization's email and Internet system comply with all organization policies and do not disclose any confidential or proprietary organization - information.

Downloading

To prevent computer viruses being transmitted through the organization's email and Internet system, there is no downloading of any unauthorized software. All software downloaded is registered to the organization. Employees may contact the SPOC if they have any questions. Furthermore, a limited bandwidth is available at our business location and provided for business purposes only. Therefore streaming music and video for personal use is not acceptable.

Copyright Issues

An employee on the Foundation's email and Internet system may not transmit copyrighted materials belonging to entities other than the organization. Note that non-adherence to this

policy puts the organization in serious legal jeopardy, opening up the organization to significant lawsuits and public embarrassment. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with permission. Failure to observe copyright or license agreements may result in disciplinary action including termination. If an employee has questions about any legal issues, he/she must speak with the President & CEO before proceeding.

Privacy & Security

Electronic communications are not private. The Foundation reserves the right to monitor content at any time ensuring that the system is used for appropriate purposes. Also, no security is 100-percent hacker-proof; someone outside the organization may intercept and read your email. Routing of email is not without errors; someone other than the intended recipient may receive your email. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways. Email messages regarding sensitive matters should warn that such communications are not intended to be secure or confidential.

The organization may monitor usage patterns in its electronic communications. Reasons for monitoring are many, including cost analysis, security, bandwidth allocation, and the general management of the organization's gateway to the Internet. All messages created, sent, or retrieved over the organization's email, IM and Internet are the property of the organization and should be considered public information.

Notwithstanding previous comments regarding the organization's current intention not to monitor content, the organization reserves the right to access and monitor the content of all messages and files on the organization's email, IM and Internet system any time in the future with or without notice.

Authorized Personal Mobile Device Use Guidelines:

Some Foundation staff may be authorized personal mobile devices for work purposes. Please refer to the Foundation's BYOD Policy. Users who are authorized to utilize their personal mobile device for Foundation business use are requested to follow good security practices and agree to: using a secure pass-code to protect the device, not disabling or altering the security settings on the device, taking care to physically secure the device against theft, loss or unauthorized use, and download security applications as appropriate, turn off Bluetooth while not in use, ensure apps are purchased via a reputable vendor and are responsible for understanding the terms and conditions of those applications, and notify the Foundation if a device is lost or stolen.

Violations

Any employee who abuses the privilege of organization-facilitated access to email, the Internet or mobile device can be subject to corrective action including termination. If necessary, the organization reserves the right to advise appropriate legal officials of any illegal violations.

6. INTELLECTUAL PROPERTY POLICIES

Purpose

The purpose of intellectual property policy is to educate Foundation employees regarding the consistent, safe and legal use of organization owned information technology assets while simultaneously safeguarding employee productivity and critical Foundation business operations/assets.

Overview

All data on all media (hard or removable disks and other storage devices) are considered property of the Foundation and may not be copied, removed, deleted or otherwise disseminated to non-Foundation parties or rendered unavailable to the Foundation management. The only exception to this provision is that intellectual property necessary to carry on day-to-day business of the Foundation and authorized by Foundation management either specifically or by policy. Password protected documents are not permitted unless authorized by the President & CEO.

7. ASSET MANAGEMENT POLICIES

Purpose

The purpose of asset management policy is to safeguard Foundation employee productivity and critical Foundation business operations/assets, while reducing or eliminating financial and legal risk.

Overview

No formal Asset Management plan has been developed for the Foundation. However, the following procedures serve as the foundation for the management of critical IT systems or assets:

1. Associate each IT asset with a specific employee or area. Association for both PC and peripherals includes make, model, version / release number and serial number. Include a digital image if possible. Store this information in on the hard drive and backed up to the cloud.

2. Create and maintain an asset lifecycle (acquisition through disposal) plan that stewards assets through their useful life. Track and record the proper disposal of all IT assets no longer in use. This can be done either through donation or through contacting the local waste management authority to ensure the proper approach to discarding potentially hazardous materials.

3. The MSP will maintain Software License Keys. Any original licensed software, as well as backup copies of other purchased software, maintained by the Foundation in a software library. Users with one-of-a-kind software are encouraged to have backup copies here as well. All software will be the most current version in use. Software keys are under the control of the MSP.

8. SECURITY POLICIES

Purpose

The purpose of a security policy is to educate Foundation employees regarding the consistent, safe and legal use of organization owned information technology assets while simultaneously safeguarding employee productivity and critical Foundation business operations/assets.

Overview

No formal IT Security plan has been developed for the Foundation. However, the following procedures serve as a foundation for the protection of critical IT systems or assets:

I. Facility Level

1. Maintain a physically secure facility (e.g. guest check–in at the front desk, appropriate use of locks, Wi-Fi passwords etc.).

II. Desktop Level

1. Never disable any security settings or software features designed to protect the Foundation from either intrusions or viruses.
2. When away from the desk, or when computers are not in use, the user should: 1) utilize a password protected screensaver, 2) Lock the Desktop, or 3) log-off the network.

III. Employee Termination

1. Termination of employees: An employee should not be terminated until he/she is denied all access to the system, if possible. The employer must contact the MSP to have the terminated employee's account disabled. The employee's password must be removed from that part of the system that accesses any data or program files.
2. Restricted access after voluntary employee termination: When an employee gives notice, a review of whether to terminate or restrict access to privileged data should take place, and a decision be made within 24 hours of receiving notice.

9. DISASTER RECOVERY POLICIES

Purpose

The purpose of the disaster recovery policy is to ensure that, in case of force majeure, critical business and information assets are protected through redundancy while simultaneously readying for the expedited restoration of organization-owned information technology assets.

Overview

No formal Business Continuity plan has been developed for the Foundation. However, the following procedures, within the context of the Foundation's current technology environment, serve as immediate mitigation regarding the recovery of critical IT systems or assets:

1. Maintaining a physically secure facility (e.g. guest check–in, appropriate use of locks etc);
2. Maintenance and control of physical asset inventory;

3. Maintenance and control of Software Library.
4. Daily rotation / validation and proper identification / storage of server back-ups;
5. Daily back up of individual data to the designated server shared and private drive areas;
6. Never disable or reconfigure any security or anti-virus software settings.

10. SIGNATURE PAGE

The Alaska Community Foundation
Information Technology (IT) Policies & Procedures

I have received a copy of The Alaska Community Foundation's (the "Foundation") Information Technology (IT) Policies & Procedures. I understand that the most current version of this document is always available for my review on the shared network drive. I have discussed this document with the Foundation's management and understand my responsibilities as an employee of the Foundation.

In accordance with the Electronic Communications Guidelines, I recognize and understand that the company's Electronic Communications systems are to be used for conducting the company's business. The Foundation recognizes there will be occasional personal use, but this shall not be excessive or unreasonable.

As part of the Foundation's organization and use of the Foundation's gateway to the Internet and electronic communications system, I understand that this Acceptable Use Policy applies to me. I have read the aforementioned document and agree to follow all policies and procedures that are set forth herein. I further agree to abide by the standards set in the document for the duration of my employment with the Foundation. I understand that Internet and Electronic Communications usage may be monitored by the company to ensure compliance with the Acceptable Use Policy.

I am aware that violations of this Acceptable Use Policy may subject me to disciplinary action, up to and including discharge from employment. I further understand that my communications on the Internet and through electronic communications reflect the Foundation worldwide to our clients, peers, partners and suppliers. Furthermore, I understand that this document can be amended at any time, and I will be asked to review changes and indicate my understanding of those changes.

_____ _____

Employee's Signature Date

_____

Employee's Printed Name

cc: Employee's Personnel File

Policy Approval, Review and Revision History

Policy: Information Technology Policies & Procedures

Date	Action taken	Comments
2/16/12	Policy approved by ACF Board	
11/14/16	Policy approved by ACF Board	

Next Revision Date: 2018.11