

Alaska Airlines and Horizon Air Technology & Information Security Policy for Third Parties

Issue Date: 4/18/2011

Alaska and Horizon have a legal and ethical obligation to customers, employees, partners and shareholders who entrust us with their confidential information. Our duty is to protect information through its lifecycle – origination through authorized disposal - regardless of its storage medium (paper or electronic). Crucial to this protection is ensuring our electronic systems are available, accurate and the information they contain is not compromised.

This is why the Technology and Information Security Policy (TISP) manual is so important for all users to read, understand and follow. These policies provide you with directives that will assist the company in fulfilling its obligations and complying with existing laws and regulations. Noncompliance with these policies could have varying results: brand damage, adverse impact to the operation, significant legal penalties or fines, and the loss of revenue that is essential for the company to achieve its long term goal of providing a fair market return and a dependable place of employment.

The policies within the TISP govern such areas as email usage, Internet usage, information classification, ownership of assets, protection of technology equipment, and third party access to assets, among others. As an employee, you must be familiar with each section because those who use and support the network are the first line of defense. You play a critical role in maintaining the confidentiality and integrity of information and ensuring availability of systems.

The efforts of every employee, vendor and contractor to comply with these policies will make the difference necessary in ensuring company information is utilized for its intended purpose and to the best advantage of Alaska and Horizon.

Failure to adhere to these policies may result in disciplinary action up to and including termination and any other remedy available.

Brandon Peterson, Vice President Finance and Controller
Andy Schneider Senior Vice President, People and Customer Services
Kelley Dobbs, Vice President Human Resources and Labor Relations
Kris Kutchera, Vice President Information Technology
Aileen Cronin, Managing Director, Privacy, Security and Environmental Affairs and Associate General Counsel
Joe Sprague, Vice President, Marketing Keith Loveless, Vice President, Legal and Corporate Affairs, General Counsel and Corporate Secretary

Alaska Airlines and Horizon Air
Technology & Information Security Policy for Third Parties
Issue Date: 4/18/2011

POLICY NUMBER 1.0: INFORMATION SECURITY AND OWNERSHIP

Alaska Airlines and Horizon Air strive to protect the confidentiality of information in their possession, custody or control by maintaining reasonable safeguards to protect against the loss, misuse or unlawful disclosure.

Improper use of computer equipment or information may jeopardize the privacy of customer and employee information, business proprietary information and, in the case of violations of the law or regulations, subject Alaska or Horizon to significant penalties.

To ensure that business objectives of Alaska and Horizon are maintained, all users have a responsibility to protect information from unauthorized access, modification, disclosure, or destruction, whether accidental or intentional.

DEFINITIONS

- **Due Care:** Care that an ordinary and reasonable person would use to protect something from reasonable foreseeable harm.
- **Users:** Anyone with access to company computing resources, information or facilities. Including but not limited to contractors, independent contractors, vendors, contingent labor, partners, and employees.

1.1 INFORMATION IN ANY FORMAT IS A COMPANY ASSET

All information or products that are developed, generated, printed, filmed, typed, written, stored or verbally communicated by a user in the course of their employment regardless of storage medium, is a company asset and is the exclusive property of Alaska or Horizon. Information or data should not be provided to any other organization, individual or entity unless Information Security or Legal has signed a specific written agreement for release.

1.2 ALL COMPUTING RESOURCES ARE COMPANY-OWNED

All company owned computing resources including hardware and software are the property of Alaska and Horizon and must be surrendered upon separation of employment or contract with the company.

1.3 LIMITATIONS ON EXPECTATIONS OF PRIVACY

Users have no expectation of personal privacy rights in any information or products that are created, received or sent using Alaska or Horizon owned equipment or software in electronic or hard-copy form. Alaska and Horizon reserves the right to access, retrieve, copy, store, and read any information composed, sent, or received through its computing systems or in hard-copy form. Using reasonable business judgment, Alaska and Horizon may disclose information to law enforcement or regulatory agencies as required. Furthermore, Alaska and Horizon are not responsible for inadvertent release or disclosure of non-company information or data that exists or transits company systems.

1.4 USERS OBLIGATED TO PROTECT ALL INFORMATION

To ensure business objectives and customer confidence, all Users have a responsibility to protect information from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional. In particular, Users must exercise due care to protect [Restricted](#) and [Confidential](#) classified information in either hard-copy or electronic format for which they have knowledge and access.

Alaska Airlines and Horizon Air Technology & Information Security Policy for Third Parties

Issue Date: 4/18/2011

Responsibilities

- **Officers, Managing Directors and Directors** of Alaska and Horizon are required to employ internal controls designed to safeguard company assets, including business information.
- **Managers and Supervisors** have an obligation to ensure that all users understand and comply with Alaska and Horizon security policies as well as all applicable laws and regulations.
- **All Users** are responsible for protecting information according to the policies of Alaska and Horizon.

1.5 REPORTING UNAUTHORIZED ACCESS

Users are responsible to immediately notify their manager, Privacy and Security or the IT Help Desk in the event they suspect or gain knowledge of any breach or misuse of company, customer or employee information. There are legal reporting obligations if the information contains any Personally Identifiable Information (PII), e.g. name, credit card and social security number.

POLICY NUMBER 2.0: INFORMATION PROTECTION AND CLASSIFICATION

Information is an asset and will be protected throughout its lifecycle - from origination through authorized disposal whether in hard-copy or electronic format. Alaska Airlines and Horizon Air strive to appropriately maintain records that are generated in the course of its business and discard them when they are no longer necessary. Often the storage, use, transmission and destruction of this information is regulated by laws and/or regulations.

INFORMATION CLASSIFICATION

- **Public:** Available to the general public and intended for distribution outside Alaska and Horizon. It may be freely disseminated without potential harm. Examples are brochures, employment opportunities, press releases and publications to customers.
- **Internal Use:** For use only within Alaska and Horizon. The unauthorized disclosure, modification or destruction of this information is not expected to adversely impact Alaska or Horizon's customers, employees or business partners. Examples are procedures, employee training materials and internal policy manuals.
- **Confidential:** Applies to information that is intended for use within Alaska and Horizon that should not be released externally without proper authorization. Disclosure would likely have an adverse impact upon Alaska and Horizon customers, employees, business partners or shareholders. Examples are certain financial data and vendor contracts, internal company phone book, and financial information related to stock strategy.
- **Restricted:** Applies to the most sensitive business information that is intended for use only within Alaska and Horizon, including all financial data that has not been publicly disclosed by an authorized source. Disclosure would adversely impact Alaska and Horizon's customers, employees and partners. Examples are new city destinations, strategic corporate plans, payroll and personnel records, social security numbers, social insurance number (Canada), IMSS (Mexico), credit card information, legal information, and proprietary information.

Alaska Airlines and Horizon Air Technology & Information Security Policy for Third Parties

Issue Date: 4/18/2011

- **Authorized Employee & Contractor:** An employee or contractor who has a legitimate and necessary business purpose for accessing information.

2.1 ALL INFORMATION HAS AN OWNER

Information must have a primary owner who is typically from the department or division directly associated with the information.

2.2 INFORMATION ROLES AND RESPONSIBILITIES

Responsibility and roles with respect to information are:

- **Owner:** Senior level business management who is primarily responsible for determining appropriate use of information and access criteria and privileges
- **Custodian:** Typically a non-business group that provides for the safekeeping, processing and recovery of information, i.e., Information Technology Services (IT).
- **User:** Anyone with access to company computing resources, information or facilities. Including but not limited to contractors, independent contractors, vendors, contingent labor, partners, and employees. Individuals agree to fully comply with all applicable policies.

2.3 CLASSIFICATION DETERMINES HOW INFORMATION IS HANDLED

A classification system (i.e., Public, Internal, [Confidential](#), or [Restricted](#)) will be employed to indicate the information's sensitivity, criticality and value to Alaska and Horizon and the safeguards required to protect it, regardless of the media on which it is stored. The information owner is responsible for classifying their information.

2.4 STORE CONFIDENTIAL ELECTRONIC INFORMATION ON CORPORATE SERVERS

Private information that is classified as [Restricted](#) or [Confidential](#) – including SSN and credit card data – may only be stored on Alaska's corporate servers. This information, whether accessed remotely (VPN) or from within a company facility, must not be copied, moved or stored on a user's local PC or laptop hard drive nor onto any removable electronic media, (examples include CDs, DVDs, USB drives, Smartphones and iPods).

2.5 SECURE CONFIDENTIAL HARD-COPY INFORMATION

Confidential information in hard-copy form that is classified as [Restricted](#) or [Confidential](#) – including SSN and credit card data – should be secured in a locked file cabinet when not in use. If a User is printing or receiving private information to a shared printer or fax machine, the content should be immediately picked up or the printer or fax machine should be secured from others who aren't entitled to such information.

2.6 DESTRUCTION OF INFORMATION

When information is disposed of, Alaska and Horizon users will take reasonable steps to securely destroy or arrange for the secure destruction of records. [Confidential](#) and [Restricted](#) hardcopy documents must be disposed of through cross-cut shredding or use of Alaska and Horizon commercial shred bins, ex. Iron Mountain. Electronic media, including CDs, DVDs, USB Drives, and hard drives must be permanently deleted through an electronic wiping process, or physically destroyed to ensure the information is permanently unreadable.

POLICY NUMBER 3.0: USER ACCESS CONTROLS AND PASSWORDS

Alaska Airlines and Horizon Air Technology & Information Security Policy for Third Parties

Issue Date: 4/18/2011

Appropriate logical access control to Alaska Airlines and Horizon Air's information and computing systems is critical in maintaining confidentiality, integrity, accountability and availability of customer, employee, partner and proprietary information.

3.1 SYSTEM ACCESS AUTHORIZATION

Access rights to information and services are granted by the system administrator. Access is based on need-to-know in connection with job responsibilities and consistent with Alaska and Horizon policies and procedures. Users that find they have inappropriate or unauthorized access should report it to the IT Help Desk so access can be removed.

3.2 PASSWORD CONSTRUCTION REQUIREMENTS

Passwords used for authentication will be complex (alpha and numeric with special characters optional) non-repeating, uncommon, and changed periodically as follows:

Requirements

- Use a minimum password length of 8 characters
- Include a minimum of one upper case and one numeric character
- Change passwords every 90 days
- Do not repeat a password for 24 iterations
- Do not use predictable sequences, e.g., customer01, customer02, etc
- Do not use dictionary or common names

3.3 SHARING ACCOUNTS NOT ALLOWED

Users must not transfer or share their account logon name or password with anyone. The exceptions to this policy are those authorized individuals whose business function requires it and the PET application as allowed by the Pass policy.

3.4 GENERIC ACCOUNTS NOT ALLOWED

Common use accounts are not allowed except under certain circumstances with appropriate compensating controls. Requests are made through the IT Help Desk.

3.5 LOCKING UNATTENDED COMPUTERS

Users are expected to log off or lock their computers before they leave the computer for any reason. Users should activate the operating system screen-saver to password protect after 15 minutes of inactivity. The only exceptions to this are multi-user kiosks or auto-login workstations approved by IT.

3.6 ACCESSING COMPUTER AFTER USER ACCOUNT LOCKOUT

After a set number of failed logon attempts, a User's network account will automatically lock. Access will be restored after contacting the IT Help Desk who will validate the identity of the user and unlock the account.

3.7 LOGON BANNER NOTIFICATION OF OWNERSHIP RIGHTS

Alaska and Horizon's workstation logon banner notifies users - both authorized and unauthorized - of Alaska and Horizon's ownership and rights over the computing technology and information being utilized by the user. Login to Alaska and Horizon systems presumes consent to the terms posted in the banner.

Alaska Airlines and Horizon Air Technology & Information Security Policy for Third Parties

Issue Date: 4/18/2011

3.8 PASSWORD STORAGE

Passwords are confidential information and may not be disclosed to anyone for any purpose. The exceptions to this policy are those authorized individuals whose business function requires it and the PET application as allowed by the Pass policy. Maintaining passwords in printed or electronic form, including storing passwords in an automated logon process, is prohibited, unless stored to a personal network drive (typically H drive).

3.9 PASSWORD INTEGRITY

Passwords for company systems should be unique to these systems. Users and contractors may not re-use those passwords for personal use in non-company systems.

POLICY NUMBER 4.0: THIRD PARTY ACCESS TO COMPUTER ASSETS

Granting access to Alaska Airlines and Horizon Air information by Third Parties (Vendors, Consultants and Contractors) increases risk of information loss. Due care requires that specific protections be in place to ensure information, especially [Restricted](#) and [Confidential](#) information, is not intentionally or inadvertently breached.

4.1 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENTS

All Third Parties – vendors, consultants, and contractors – will sign a Non-Disclosure agreement (Alaska or Horizon as applicable) and Confidentiality and Technology Acceptance Agreement committing to:

- Adhere to Alaska and Horizon's security policies and procedures
- Take adequate measures to protect and safeguard Alaska and Horizon's [Restricted](#) and [Confidential](#) information
- Signing and executing the agreement prior to obtaining access to any Alaska or Horizon information.

4.2 THIRD PARTY CONTRACT TERMS

Third party contracts for vendors or contractors requiring access to Alaska/Horizon data must include the Data Security Agreement or equivalent Confidentiality Agreement. The contract must be signed by the vendor or contractor before access is granted to Alaska/Horizon data and premises

4.3 THIRD PARTY IT RISK ASSESSMENT

All third party vendors who transmit, process or store Alaska/Horizon information are required to complete and/or pass an IT Risk third party assessment prior to initial engagement and on a renewal basis. An additional assessment should be performed prior to a change in the type of data they transmit, process or store.

4.4 LIMITATIONS ON INFORMATION REMOVAL FROM COMPUTING EQUIPMENT

Third parties will not remove or copy Alaska or Horizon [Restricted](#) or [Confidential](#) classified information on any media, including but not limited to email, hard disk drives, floppy drives, CDs, DVDs, smartphone's or thumb drives. Approved methods of transmission are encrypted media or secure FTP. Contact IT Risk Management for further guidance.

POLICY NUMBER 5.0: MONITORING, AUDIT AND COMPLIANCE

To ensure compliance with Alaska Airlines and Horizon Air's policy herein and with International, Federal and State Laws

Alaska Airlines and Horizon Air
Technology & Information Security Policy for Third Parties
Issue Date: 4/18/2011

5.1 LEGAL AND ETHICAL USE

Inappropriate material may not be created, accessed, archived, stored, distributed, edited or recorded using company resources. Inappropriate material includes but is not limited to offensive jokes, pornography, sexist remarks, racist remarks, defamatory remarks, obscene remarks, threats, harassment, impersonation, gambling, chain letters, pirated software, and solicitations.

Further, access to the Internet from the Alaska or Horizon network shall not be used for any purpose in violation of law or regulation, including but not limited to the pirating of software, gambling, or other activities damaging to the reputation of Alaska or Horizon.

5.2 COMPLIANCE WITH LEGAL REQUIREMENTS

Alaska and Horizon computing resources may only be used for lawful purposes. Transmission, distribution, or storage of any information, data, or material in violation of International, Federal, or State law is prohibited. This includes, but is not limited to, material protected by copyright, trademark, or any other statute. Alaska and Horizon reserves the right to remove illegal material from its computing network and services at any time.

5.3 LAW SUPERSEDES POLICY

Users shall manage company information according to the policies in the TISP, except when the policies are inconsistent with applicable law or legal requirements. In this event, users shall take no action contrary to law or legal requirement and immediately contact the Legal Division.

5.4 MONITORING OF ELECTRONIC COMMUNICATION AND INTERNET USAGE

Alaska and Horizon reserve the right to monitor and / or review, at any time, any electronic communication created, sent, or received via its computers, networks, and / or email systems or any Internet usage via the company network. Webmail transmitted via the company network is subject to the same general email policy found herein. The company will not and cannot guarantee the confidentiality of any communications made using a webmail service, including those communications which may be privileged. The use of encryption, the labeling of a communication as private, the deletion of a communication, or any other such process or action, shall not diminish the company's rights in any manner.

5.5 MONITORING FOR UNAUTHORIZED NETWORK DEVICES AND SOFTWARE

The company will monitor the network and attached workstations for unauthorized connectivity devices and software and remove them without notice. Connectivity devices include but are not limited to non-company laptops, routers, access points, smart phones, etc.

5.6 AUDITING TECHNOLOGY USE

Periodic audits will be conducted to ensure compliance with the requirements outlined in this policy