



INFORMATION SECURITY POLICY

Purpose

It is the established policy of Alto Aerospace Ltd to operate within the requirements of a documented Information Security Policy statement as a means to comply with all statutory, regulatory and contractual requirements, and, to protect the interests, property and information of the company, and of its clients and employees, against threats or loss.

Information is a major asset that Alto Aerospace has a responsibility and requirement to protect. Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow, and the physical computer equipment used to access them.

The following policy details the basic requirements and responsibilities for the proper management of information assets at Alto Aerospace. The policy specifies the means of information handling and transfer within the Business. This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

Scope

This Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the Organisation who have access to Information Systems or information used for Alto Aerospace purposes.

Acceptable Use

- Alto Aerospace's proprietary information stored on electronic and computing devices whether owned or leased by Alto Aerospace, the employee or a third party, remains the sole property of Alto Aerospace. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Alto Aerospace's proprietary information.
- You may access, use or share Alto Aerospace's proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Alto Aerospace may monitor equipment, systems and network traffic at any time, per Alto's Audit Policy.
- Alto Aerospace reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Clean Desk

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the workday.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Emails

- All use of email must be consistent with Alto Aerospace's policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Alto Aerospace email accounts should be used primarily for Alto Aerospace business related purposes; personal communication is permitted on a limited basis, but non-work-related commercial use is prohibited.
- All Alto Aerospace data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- The Alto Aerospace email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any employee should report the matter to their supervisor

immediately.

- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Alto Aerospace business, to create or memorialize any binding transactions, or to store or retain email on behalf of Alto Aerospace. Such communications and transactions should be conducted through proper channels using approved documentation.
- Alto Aerospace employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- Alto Aerospace may monitor messages without prior notice. Alto Aerospace is not obliged to monitor email messages.

Ethics

- Executive Commitment to Ethics

- Senior leaders and executives within Alto Aerospace must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- Executives must have an open-door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- Executives must disclose any conflict of interests regard their position within Alto Aerospace.

- Employee Commitment to Ethics

- Alto Aerospace employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- Every employee needs to apply effort and intelligence in maintaining ethics value.
- Employees must disclose any conflict of interests regard their position within Alto Aerospace.
- Alto Aerospace will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.
- Alto Aerospace will not tolerate harassment or discrimination.
- Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.
- Alto Aerospace will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
- Employees at Alto Aerospace should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- Employees should consider the following questions to themselves when any behaviour is questionable:
 - Is the behaviour legal?
 - Does the behaviour comply with all appropriate Alto Aerospace's policies?
 - Does the behaviour reflect Alto Aerospace's values and culture?
 - Could the behaviour adversely affect company stakeholders?
 - Would you feel personally concerned if the behaviour appeared in a news headline?

- Could the behaviour adversely affect Alto Aerospace if all employees did it?

Password Construction Guidelines

- Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:
 - Contain eight characters or less.
 - Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
 - Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
 - Are some version of “Welcome123” “Password123” “Changeme123”

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorized. Whenever possible, also enable the use of multifactor authentication.

Password Protection

- Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Users must use a separate, unique password for each of their work-related accounts.
- Users may not use any work-related passwords for their own, personal accounts.
- Passwords should be changed only when there is reason to believe a password has been compromised.
-

- Password Protection

- Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, Confidential Alto Aerospace information.
- Passwords must not be inserted into email messages.
- Passwords may be stored only in “password managers” authorized by the organization.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Technology Equipment Disposal

- This policy on disposal covers all data or information held by Alto Aerospace whether held digitally or electronically on IT equipment or as manual records held on paper or in hard copy.
- Where information is held on IT equipment, it is the policy of Alto Aerospace that such equipment will be assumed to hold sensitive information and that all information residing on such equipment must be disposed of securely.
- Alto Aerospace supports policies which promote sustainability and take account of environmental impact. Alto Aerospace will therefore support recycling or sustainable redeployment in the disposal of IT equipment if the information held on the equipment is irretrievably and securely destroyed prior to the disposal of the equipment.
- WEEE: IT equipment must also be disposed of in line with the EU Waste Electrical and Electronic Equipment (WEEE) Directive and the UK Waste Electrical and Electronic Equipment Regulations 2013.
- Copyright: software must be disposed of in line with copyright legislation and software licensing provisions.
- Information and data held in paper or hard copy which contain sensitive information shall be irretrievably destroyed in a way in which the information cannot be reconstituted, by shredding, pulping or incineration.
- The process leading to and the process of shredding, pulping or incinerating such information shall be carried out securely.
- Since the policy default is that all IT equipment which stores, or processes data will be deemed to hold sensitive data, then all such IT equipment will undergo appropriate physical destruction, or an appropriate data overwrite procedure which irretrievably destroys any data or information held on that equipment.
- Where an overwrite procedure fails to destroy the information irretrievably, the equipment shall be physically destroyed to the extent that the information contained in it is also irretrievably destroyed.
- All IT equipment awaiting disposal must be stored and handled securely.
- Photocopiers and printers used or owned by Alto Aerospace may have a data storage capacity. Where such IT equipment contains information or data, the disposal of such equipment must have due regard to this policy.
- Staff holding Alto Aerospace data on IT equipment should routinely dispose of the data when it is no longer required to be held for legal or contractual purposes or is no longer necessary for the business purpose for which it was originally created or held.

Social Media

Alto Aerospace recognises that employees' personal social media accounts can generate several benefits. For instance:

- Staff members can make industry contacts that may be useful in their jobs
- Employees can discover content to help them learn and develop in their role
- By posting about the company, staff members can help to build the business' profile online.

Acceptable use:

- Employees may use their personal social media accounts for work-related purposes during regular hours but must ensure this is for a specific reason (e.g. competitor research). Social media should not affect the ability of employees to perform their regular duties.
- Use of social media accounts for non-work purposes is restricted to non-work times, such as breaks and during lunch.

Users must not:

- Create or transmit material that might be defamatory or incur liability for the company.
- Post message, status updates or links to material or content that is inappropriate.

(Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone based on race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.)

- Use social media for any illegal or criminal activities.
- Send offensive or harassing material to others via social media.
- Broadcast unsolicited views on social, political, religious or other non-business-related matters.
- Send or post messages or material that could damage [company name]'s image or reputation.
- Interact with Alto Aerospace's competitors in any ways which could be interpreted as being offensive, disrespectful or rude. (Communication with direct competitors should be kept to a minimum.)
- Discuss colleagues, competitors, customers or suppliers without their approval.
- Post, upload, forward or link to spam, junk email or chain emails and messages.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Policy statement

Alto Aerospace will ensure the protection of all information assets within the custody of the Business.

High standards of confidentiality, integrity and availability of information will always be maintained.

Risks

Alto Aerospace recognises that there are risks associated with users accessing and handling information in order to conduct official business.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Application / Compliance

The Information Security Policy is maintained by audit and review, and by the methods described in the quality manual, in order to provide effective assurance that all aspects of company, employee and customer specified security requirements are being implemented.

The policy applies to all employees employed by Alto Aerospace, as well as all employers employed by a contractor or sub-contractor who perform services directly or indirectly for Alto Aerospace on a regular ongoing basis.

Review and Revision

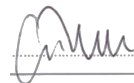
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Compliance Monitoring Manager

Signed on: 17th January 2019



Chris Yendell
Managing Director



Giles Trotter
Managing Director