

# Security Plan

## Kitty Hawk Aeronautics

---

*Version 1.0*  
*20 February 2010*

### **Introduction**

#### **Purpose of the IT Security Program**

The purpose of the IT security program is to protect the physical and intellectual assets of Kitty Hawk Aeronautics (KHA) while ensuring that legitimate users of KHA IT resources have access to the information they need when they need it and that the information has not been compromised or tampered with.

#### **Principles of IT Security**

Special Publication 800-27 by the National Institute for Standards and Technology identifies the principles of IT security as the following:

1. Establish a sound security policy as the “foundation” for design.
2. Treat security as an integral part of the overall system design.
3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
4. Reduce risk to an acceptable level.
5. Assume that external systems are insecure.
6. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
7. Implement layered security (ensure no single point of vulnerability).
8. Implement tailored system security measures to meet organizational security goals.
9. Strive for simplicity.
10. Design and operate an IT system to limit vulnerability and to be resilient in response.
11. Minimize the system elements to be trusted.
12. Implement security through a combination of measures distributed physically and logically.
13. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
14. Limit or contain vulnerabilities.
15. Formulate security measures to address multiple overlapping information domains.
16. Isolate public access systems from mission critical resources (e.g., data, processes, etc.)
17. Use boundary mechanisms to separate computing systems and network infrastructures.
18. Where possible, base security on open standards for portability and interoperability.
19. Use common language in developing security requirements.

20. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
21. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
23. Use unique identities to ensure accountability.
24. Implement least privilege.
25. Do not implement unnecessary security mechanisms.
26. Protect information while being processed, in transit, and in storage.
27. Strive for operational ease of use.
28. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
29. Consider custom products to achieve adequate security.
30. Ensure proper security in the shutdown or disposal of a system.
31. Protect against all likely classes of “attacks.”
32. Identify and prevent common errors and vulnerabilities.
33. Ensure that developers are trained in how to develop secure software.

The policy described in this document attempts to implement these principles.

### **Critical Success Factors**

In their 2004 report, *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management*, the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) defines Critical Success Factors (CSFs) as factors that influence and enable the accomplishment of enterprise strategic goals and objectives. In the area of security, identifying the CSFs are essential to ensuring that the security strategy enables the enterprise mission and aligns with the organizational strategic plan. Likewise, security activities support the successful accomplishment of operational activities. The problem is that CSFs can be difficult to identify since they often don't become apparent until a situation occurs that places accomplishment of enterprise goals at risk. For this reason, the CSFs must be constantly evaluated and adjusted.

Given the caveat above, the following are some of the CSFs that have been identified to support KHA's strategic goal to expand its commercial aviation presence into Europe and Asia, while continuing to expand its government projects for the DoD and NASA.

- Government data and resources (such as the NIPRnet node and F-18 test station) must be protected from compromise.
- Customer data (especially proprietary and financial data) must be protected from compromise and misuse.
- Employee and customer personal data must be protected from unauthorized disclosure.
- KHA and customer assets must be protected from damage and loss.

## Intended Outcomes

The intended outcomes for the KHA security program are:

- Accurate information will be available to any authorized user of that information, when they need it.
- Unauthorized users will not be able to access, modify, or deny use of IT resources.
- Customers will be able to entrust their data and resources to KHA, knowing they will be protected.
- The KHA security program will enable the achievement of the KHA 2007-2010 Strategic Plan.

## Performance Measures

No security measures can be 100% effective, which means security activities need to be focused on those areas of the enterprise that contain the most sensitive resources, while also attempting to protect all of the enterprise resources. Specific security performance measures by division are still being developed as the result of an initiative by the CIO. The current plan calls for the performance measures to all be identified and tracking mechanisms in place by July of this year.

## Policy

### Executive Guidance

The goals identified in the KHA 2007-2010 Strategic Plan are as follows:

- Increase profit by at least 7% per year.
- Establish a customer base in Asia/Europe for the Commercial Aviation line of business.
- Establish a “General Aviation Systems” line of business.
- Control costs by establishing activity based cost accounting in all lines of business.
- Improve the value of investments in information technology.

As noted in the paragraph on CSFs, these enterprise goals are the basis for the security CSFs.

### Technical Guidance

NIST SP 800-27 provides guidance on the engineering principles for IT security.

CMU/SEI-2004-TR-010 provides guidance on applying CSFs to enterprise security.

### Applicable Law and Regulations

DoDD 8500.1 directs the use of information assurance (IA) measures for DoD systems. DoDI 8500.2 provides implementation instructions for IA measures.

The Privacy Act of 1974 requires the protection of sensitive personal information for employees and customers of KHA.

## Standards

TBD

## Reporting Requirements

### IT Security Program Roles and Responsibilities

The KHA Security Office reports directly to the Chief Information Officer (CIO), Susan Martinez. The CIO establishes the policies that govern the use, creation, maintenance, and disposal of all IT resources owned and operated by KHA. The Security Office personnel implement the policy, train users of the IT resources about security policies and practices, and advise the CIO on matters of security policy.

The Security Office has also been tasked by the CIO to work with the Chief Architect at KHA, Robert Osborn, to ensure that security is considered and integrated into all levels of the KHA enterprise architecture.

Ultimately, security is the responsibility of every user of KHA IT resources. The Security Office provides annual training and security updates on a quarterly and ad hoc (as emerging security threats require) basis to all registered users of KHA IT resources. All users must be registered to gain access to KHA IT resources.

### IT Security Program Schedule and Milestones

The security program is ongoing. As mentioned above, the Security Office provides annual, quarterly, and as-needed security training. It also complies with any externally directed events, such as DoDI 8500.2 security assessments required for the DoD systems that the Defense Systems Division is working with, such as NIPRnet and any system developed by the division that needs to operate on the Global Information Grid (GIG).

There is an initiative directed by the KHA Chief Executive Officer, Dwight Hendricks, to implement the Information Technology – Common Operating Environment (IT-COE) for all front and back office applications in KHA. The Security Office will be involved in the planning and implementation of this initiative throughout the lifecycle of the project. This plan will be updated to reflect the milestones associated with the IT-COE initiative as the enterprise plan is developed. The Security Office is currently working with the Chief Architect in the development of the security elements of the enterprise architecture related to the IT-COE initiative.

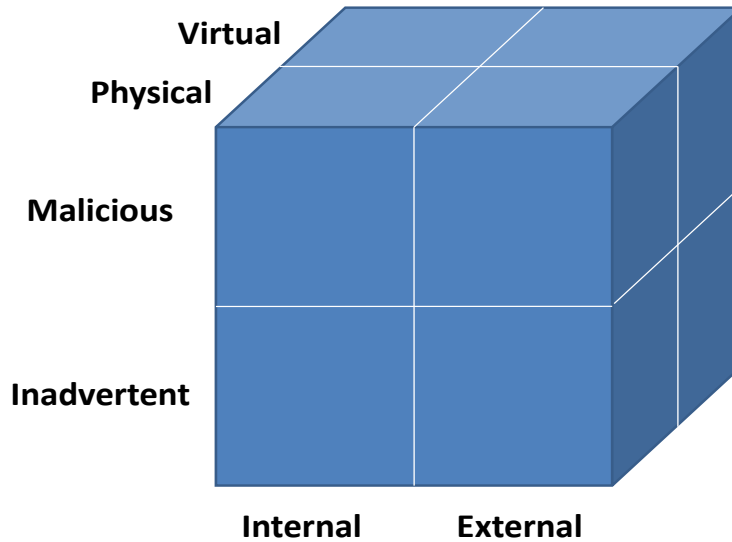
### IT Security Incident Reporting

Incidents (or suspected incidents) must be reported to the Security Office within 8 hours of their detection. The Security Office intranet site and the annual and quarterly training materials have the detailed incident reporting procedures; including contact numbers, email addresses, and a fillable web form.

## Concept of Operations

### IT Security Threat Summary

IT security threats fall into a matrix, as shown below:



Analysis of the threats and mitigation strategies for them is located in the Security Solutions Descriptions (artifact SP-2 in the EA<sup>3</sup> framework).

### IT Security Risk Mitigation

TBD

### Integration with Enterprise Architecture

TBD

### Component/System Security Plans

TBD

## Security Program Elements

### Information Security

Described in detail in the Security Solutions Descriptions.

### Personnel Security

Described in detail in the Security Solutions Descriptions.

## **Operational Security**

Described in detail in the Security Solutions Descriptions.

## **Physical Security**

Described in detail in the Security Solutions Descriptions.

## **Standard Operating Procedures**

### **Test and Evaluation**

Test and evaluation procedures and results for each system utilized by KHA are in section 3 of the System Accreditation Document for that system. (This is artifact SP-3 in the EA<sup>3</sup> framework.)

### **Risk Assessment**

The system risk assessment for each system utilized by KHA can be found in section 2 of the System Accreditation Document for that system.

### **Certification and Accreditation**

The certification and accreditation for each system utilized by KHA is documented in the System Accreditation Document.

### **Disaster Recovery/Continuity of Operations**

Disaster Recovery procedures are documented in the Disaster Recovery Plan (artifact SP-5 in the EA<sup>3</sup> framework).

Continuity of Operations plans are documented in the Continuity of Operations Plan (COOP – artifact SP-4 in the EA<sup>3</sup> framework.)

### **Records Protection and Archiving**

All records must be protected from unauthorized access and modification. They must also be archived to prevent data loss or corruption. The specific approach to data protection and archiving varies by system and line of business, since various systems will have different protection and archiving mechanisms and the protection and archiving requirements will vary, depending on the line of business (DoD requirements will not be the same as NASA requirements, for example). The requirements for each system are documented in the System Accreditation Document for that system.

### **Data Privacy**

Data privacy must comply with regulatory requirements established by the Privacy Act of 1974, since KHA is based in the United States. The details for data privacy are contained in the Data Privacy Plan in the KHA EA repository.

### **IT Security Training and Awareness**

All KHA IT users must successfully complete initial, annual, and quarterly security training. The Security Office also provides as-needed training and notices for newly identified security threats.

# Appendix A

## Inventory of IT Components

### Front Office IT Systems

#### Commercial Aviation Systems Division

- CAD/CADCAM v7.1
- Production Plant Monitoring System v4.2

#### Defense Systems Division

- GIG Broadband System IX
- NIPRNet (Node)
- USN F-18C UHF/VHF EMI-EMC Test System

#### Space Systems Division

- NASA Standards & Design System II
- USAF GeoTalk System
- NASA Mars Lander Communications System (Node to JPL and Houston Center)

#### Research and Development Division

- KHA Avionics Design & Testing System
- NASA Next-Generation Space Shuttle Avionics Program

### Back Office IT Systems

#### Finance and Administration Division

- PRISM Accounts Receivable/Payable
- SAP General Ledger
- SAP HR Module

#### Technology Support Division

- LAN
  - Gigabit Ethernet (within all operating sites)
  - CA UniCenter
  - Remedy Help Desk
- WAN
  - T-3 Dedicated Data Circuits (connect all operating sites)
- PBX
  - Nortel Meridian SL-100
- Servers
  - Linux Print and File Servers (dual clustered/mirrored units at all operating sites)
- Desktop PCs
  - Dell Optiplex

- Laptop PCs
  - Dell 630
- PDAs
  - Blackberry 8330 Curve
  - Blackberry Enterprise Server
- Standard Desktop Image
  - Microsoft Windows XP
  - Microsoft Office 2007
  - Microsoft Exchange 2007
  - Adobe Acrobat
- Collaboration
  - Microsoft SharePoint 2007
  - NetMeeting
  - GoToMeeting
- Web
  - Microsoft IIS Servers
  - Apache Web Servers
  - Microsoft Internet Explorer 2007
  - Barracuda Firewalls
- Security
  - Symantec AV (desktop/laptop)
  - Network IDN
  - CA UniCenter
  - Cisco VPN

### **Contracts and Legal Division**

- LEXUS/NEXUS Law Reference v4.8
- CA PRISM Contracting System v6.1

### **Shipping and Receiving Division**

- Pitney Bowes Shipping Center v3.5 (Node)
- FedEx Tracking System (Node)
- KHA Warehouse Inventory System
- Intermec Barcode Readers/Database v2.42

**Appendix B**  
**Definitions of IT Security Terms**

TBD

## **Appendix C**

### **List of Acronyms**

CEO	Chief Executive Officer
CIO	Chief Information Officer
CMU	Carnegie Mellon University
COOP	Continuity of Operations Plan
CSF	Critical Success Factor
DoD	Department of Defense
EA	Enterprise Architecture
GIG	Global Information Grid
IA	Information Assurance
IT	Information Technology
KHA	Kitty Hawk Aeronautics
NASA	National Aeronautics and Space Administration
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute for Standards and Technology
SEI	Software Engineering Institute
TBD	To Be Determined

## **Appendix D**

### **IT Security References**

#### **Government**

DoDI 8500.2-H  
6 February 2003

Information Assurance (IA) Implementation

NIST SP 800-27  
21 March 2001

Engineering Principles for IT Security

#### **Non-Government**

CMU/SEI-2004-TR-010  
July 2004

The Critical Success Factor Method: Establishing a Foundation for  
Enterprise Security Management