# Purpose

Argus is the information security management system implemented at NSCL’s Electronics Department. The purpose of this standard is to define the terms used in Argus’ documents.

# Scope

This standard is applicable to all documents related to Argus.

# Definitions

# Standard Statement

Most of the definitions are borrowed from [1], [2], [3], and [4].

|  |  |
| --- | --- |
| Term | Definition |
| Area Manager | A role that is responsible for the operation of a section of the NSCL facility. |
| Area of Concern | A descriptive statement that details a real-world condition or situation that could affect an information asset in your organization |
| Argus | Name of the *ISMS* implemented at the Electronics Department of NSCL |
| Asset | An asset is something of value to the enterprise. Assets are used by organizations to achieve goals, provide a return on investment, and generate revenue. The overall value of the organization can be represented collectively by the value of its assets. There are many types of assets, including:   * information * software, such as a computer program * physical, such as computer * services * people, and their qualifications, skills, and experience * intangibles, such as reputation and image |
| Attack | Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an *asset* |
| Authentication | Provision of assurance that a claimed characteristic of an entity is correct |
| Authenticity | Property that an entity is what it claims to be |
| Availability\*\* | The property of being accessible and usable upon demand by and authorized entity. |
| Business continuity | *Processes* and/or *procedures* for ensuring continued business operations |
|  |  |
| Category I, II, and III machines |  |
|  |  |
| Confidentiality\*\* | The property that information is not made available or disclosed to unauthorized individuals entities, or processes. |
| Control\* | Means of managing *risk*, including *policies*, *procedures*, *guidelines*, practices or organizational structures, which can be administrative, technical, management, or legal nature. |
| Control objective | Statement describing what is to be achieved as a result of implementing *controls* |
| Corrective action | Action to eliminate the cause of a detected nonconformity or other undesirable situation |
| Critical Information Asset | Critical information assets are the most important assets to an organization. The organization will suffer an adverse impact if   * a critical asset is disclosed to unauthorized people * a critical asset is modified without authorization * a critical asset is lost or destroyed * access to a critical asset is interrupted   For Electronics Department, information classified as Class I through Class IV is deemed critical (see R02 Information Classification document). |
|  |  |
| Guideline\* | A description that clarifies what should be done and how, to achieve the objectives set out in policies. |
| Human asset |  |
| Impact | The effect of a threat on an organization’s mission and business objectives |
| Impact statement | A descriptive statement thatdetails how the organization is impacted when a threat scenario is realized. The impact statement is the consequence of the realization of a threat scenario |
| Impact Value | A qualitative value assigned to describe the extent of impact to an organization when a threat scenario and resulting impact is realized. The impact value is derived from the risk measurement criteria. |
| Information Asset | An information asset can be described as information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information. These assets can exist in physical form (on paper, CDs, or other me-dia) or electronically (stored on databases, in files, on personal computers) |
| Information Classification | Grouping of information assets based on their sensitivity or criticality. See *R02 Information Classification* document. For the current classification |
| Information asset container | An information asset container is where information assets are stored, transported, or processed. It is a place where an information asset “lives.” Containers generally include hardware, software, application systems, servers, and networks (technology assets), but they can also include items such as file folders (where information is stored in written form) or people (who may carry around important information such as intellectual property). They can also be both internal and external to an organization. |
| Information Asset Custodian | Custodian of information assets refers to the roles (and indirectly to the individuals who fill in the roles) in the organization that have the responsibility to protect information assets that are stored, transported, or processed in containers. In other words, custodians accept responsibility for the information assets that live in containers that they manage and ensure the protection of the assets per the owner’s requirements. |
| Information Asset Owner | Owners of information assets are those roles (and indirectly those individuals who fill in the roles) that have primary responsibility for the viability, survivability, and resiliency of an information asset. They set security requirements for the asset and ensure that proper protection strategies have been implemented in the organization to meet these requirements. |
| Information Asset Profile | A representation of an information asset describing its unique features, qualities, characteristics, and value. |
| Information Processing Facility\* | Any information processing system, service or infrastructure, or the physical locations housing them |
|  |  |
| Information security\* | Preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved. |
| Information Security Board |  |
| Information security event\* | An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. |
| Information security incident\* | Single or a series of unwanted or unexpected *information security events* that have a significant probability of compromising business operations and threatening information security |
| Information security incident management | Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents |
| Information Security Management System (ISMS)\*\* | That part of the overall management system, based on a business risk approach, to establish implement, operate, monitor review, maintain, and improve information security. |
| Information System |  |
| Information processing facility | An information processing facility is defined as any system,  service, or infrastructure, or any physical location that houses  these things. A facility can be either an activity or a place;  it can be either tangible or intangible. |
| Integrity\*\* | The property of safeguarding the accuracy and completeness of assets. |
| Malicious Code | Collective term for computer viruses, network worms, malware, spyware, Trojan horses, and other harmful mobile code. |
| Management system | Framework of *policies*, *procedures*, *guidelines* and associated resources to achieve the objectives of the organization |
| Mobile Code | Any software that has been transferred from outside, and is executed on the local system without explicit initiation by the user. Examples are ActiveX controls, Flash animations, Java Applets, and JavaScript scripts. |
| Mitigation approach | The way that an organization intends to address a risk. An organization has the following options: accept, mitigate, or defer.   * Accept – A decision made during risk analysis to take no action to address a risk and to accept the stated consequences. Risks that are accepted should have little to low impact on the organization. * Mitigate – A decision made during risk analysis to address a risk by developing and implementing controls to counter the underlying threat or to minimize the resulting impact, or both. Risks that are mitigated are those that typically have a medium to high impact on an organization. * Defer – A situation where a risk is neither accepted nor mitigated based on the organization’s desire to gather additional information and perform additional analysis. Deferred risks are monitored and re-evaluated at some point in the future. Risks that are deferred are generally not an imminent threat to the organization nor would they significantly impact the organization if realized |
| Mobile computing and communication facilities | Mobile devices that process information. Examples include laptops, smartphones, mobile phones, and netbooks. |
| Non-repudiation | Ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event |
| PDCA model | Plan-Do-Check-Act model |
| Physical asset |  |
| PLC | Programmable Logic Controller. |
| Policy\* | Overall intention and direction as formally expressed by management |
| Preventive action | Action to eliminate the cause of a potential nonconformity or other undesirable potential situation |
| Procedure | Specified way to carry out an activity or a *process* |
| Process | Set of interrelated or interacting activities which transforms inputs into outputs |
| Record | Artifacts stating results achieved or providing evidence of activities performed |
| Remote Access | Access to the department’s information systems from outside the NSCL premises, or over communication channels that are not under NSCL’s administrative control. |
| Removable Media | Removable media are devices that can store information and can be easily removed and taken out of office premises. These include USB or Bluetooth storage devices, smartphones, and writable CDs/DVDs |
| Residual risk | Residual risk is the risk that remains when a mitigation approach has been developed and implemented for the range of risks that affect an information asset. Residual risk that remains must be acceptable to the organization |
| Risk | A risk is the possibility of suffering harm or loss. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. A risk is composed of   * an event, * a consequence, and * uncertainty |
| Risk acceptance\*\* | Decision to accept risk. |
| Risk analysis\* | Systematic use of information to identify sources and estimate risk |
| Risk assessment\* | Overall process of risk analysis and risk evaluation |
| Risk evaluation\* | Process of comparing risk against given risk criteria to determine significance of the risk |
| Risk management\* | Coordinate activities to direct and control and organization with regard to risk. It typically includes risk assessment, risk treatment, risk acceptance, and risk communication. |
| Risk Measurement Criteria | A set of qualitative measures against which the effect of each risk on an organization’s mission and business objectives is evaluated. Risk measurement criteria define ranges of high, medium, and low impacts for an organization |
| Risk treatment | Process of selection and implementation of measures (controls) to modify risk. |
| Security requirements | The requirements that characterize how an information asset is to be protected. These are also often referred to as “security objectives.”   * Confidentiality – Ensuring that only authorized people (or systems) have access to an information asset. * Integrity – Ensuring that an information asset remains in the condition that was intended by the owner and for the purposes intended by the owner. * Availability – Ensuring that the information asset remains accessible to authorized users. |
| Senior Management | The Electronics Department Head (EEDH) and the representatives designated by EEDH as senior management. |
| Statement of Applicability\*\* | Documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS (Information Security Management System). |
| System Documentation | Set of documents that describe a system in detail, and contain sensitive information such as authorization procedures, data structures, and security architecture. |
| Technology assets | Technology assets typically describe electronic containers in which information assets are stored, transported, or processed. These assets generally include hardware, software, application systems, servers, and networks |
| Threat | A threat is an indication of a potential undesirable event. A threat refers to a situation (or scenario) in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization’s email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization’s information technology hardware). A threat is created when a threat actor exploits a vulnerability |
| Threat scenario | A threat scenario is a situation in which an information asset can be compromised. It generally consists of an actor, a motive, a means (access), and an undesired outcome. Threat scenarios are simplified ways to determine if a risk exists that could affect your information asset |
| Threat trees | A tree structure used to visually represent a range of threat scenarios. Threat trees help you to ensure that you consider a broad range of potential threats to your information asset as the basis for determining risk |
| User | A person or a system that consumes or uses the information assets of the lab (NSCL). |
| Vulnerability\* | A weakness of an *asset* or group of *assets* that can be exploited by one or more *threats*. |

# Exceptions

# References

1. ISO/IEC 27000 International Standard, Information Technology – Security Techniques –Information security management systems – Overview and vocabulary
2. ISO/IEC 27001 International Standard, Information Technology – Security Techniques –Information security management systems – Requirements
3. ISO/IEC 27002/17799 International Standard, Information Technology – Security Techniques – Code of practice for information security management
4. The OCTAVE Allegro Guidebook V1.0, Computer Emergency Response Team (CERT) Program, Software Engineering Institute, Carnegie Mellon University

# Revision History

|  |  |  |
| --- | --- | --- |
| Revision  Level | Date | Revision Changes |
|  |  |  |

# Reviews

|  |  |
| --- | --- |
| Reviewer | Review Date |
| Information Security Working Group |  |

**Approved**

**Department Head:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Approval Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Effective Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**