Information Security Regulation

Original Regulation issued on,

October 1, 2003 as Regulation #15-48

Revised Regulation issued on,

March 29, 2004 as Regulation #16-28
June 29, 2004 as Regulation #16-40
May 12, 2005 as Regulation #17-47
September 30, 2005 as Regulation #17-106
March 25, 2008 as Regulation #20-23

Japan Aerospace Exploration Agency
Information Security Regulation

Chapter 1 General Provision

Article 1 Purposes
The present set of regulations stipulates basic items, and thus it serves to protect important information owned by the Japan Aerospace Exploration Agency, an independent administrative institution (hereafter, referred to as the “Agency”), from being stolen, leaked, tampered, destroyed, erased, burned or attacked by other threats, as well as to ensure the confidentiality, integrity, and availability thereof (hereafter, referred to as “Information Security”).

Article 2 Definition
In the present set of regulations, the terms listed below shall be defined as follows:
(1) The term “Personnel” shall refer to persons to whom the Work Regulation (Regulation #15-23) and the Special Work Regulation (Regulation #15-24) apply.
(2) The term “Information” shall refer to documents, drawings, and electromagnetic records.
(3) The term “Information Systems” shall refer to a system that consists of hardware, software, a network, and storage media; by utilizing a combination of the above, operations such as recording, processing, and communicating Information can be conducted.
(4) “Reading” shall refer to disclosing a piece of Information at the reading room stipulated in Article 13, to the concerned executives or Personnel of the Agency (hereafter, referred to as the “Executives and Personnel”) as well as to external persons concerned.
(5) “Copying” shall refer to creating a copy of a piece of Information through means of the handwriting of the Executives and Personnel, use of a copier, or use of Information Systems. The resulting copy shall be referred to as “Copied Information.”
(6) “Removing” shall refer to the removal by Executives and Personnel of a piece of Information to a location outside of the storage area that is stipulated in Article 12 and placing it under his/her own control.
(7) “Lending” shall refer to entrusting by Executives and Personnel of a piece of Information to persons internal and external to the Agency for a period of time designated by the Executives and Personnel, and placing it under the control of the person.
(8) “Sending” shall refer to handing over a piece of Information to persons internal and external to the Agency and placing it under the control of the person, including its disposal.
(9) The terms “Directorates and Departments” shall refer to the headquarters and divisions of the Agency that are stipulated in Article 2-4 of the Security Regulation # 15-47.

Chapter 2 Categorization of Information
Article 3 Categorization of Information

Information owned by the Agency, the security of which must be ensured, shall be categorized as follows according to its degree of importance and risk assessment:

(1) Top Secret Information

The highest level of classification of information security. Such Information would cause exceptionally grave damage to national security or benefits if disclosed.

(2) Secret Information

A high level of classification of Information Security. Such Information would cause grave damage to national security or make it extremely difficult for the Agency to conduct its operations if disclosed.

(3) Information limited to authorized staff

If such information is disclosed it would impede the smooth implementation of operations conducted by the Agency, damage the financial assets of the Agency, violate the position of the Agency as a party to a contract, violate the benefits of the other party to a cooperative treaty or cooperative research project, or violate the legal status and benefits of the Agency and persons concerned through violating individual human rights and privacy. Thus its disclosure shall be allowed only to the following people;

a) concerned Executives and Personnel of the Agency,

b) concerned people of other organization than the Agency.

(4) Information limited to JAXA employees

If such information is disclosed, it would impede the smooth implementation of operations conducted by the Agency, damage the financial assets of the Agency, violate the position of the Agency as a party to a contract, violate the benefits of the other party to a cooperative agreement or cooperative research project, or violate the legal status and benefits of the Agency and persons concerned through violating individual human rights and privacy. Thus its disclosure shall be allowed only to the following people;

a) Executives and Personnel of the Agency,

b) concerned people of other organization than the Agency.

Chapter 3 Controlled Areas

Article 4 Categories of Controlled Areas

In order to effectively and efficiently ensure the security of corporate buildings and compounds that belong to the Agency (including annexed facilities these are hereafter collectively referred to as “Corporate Buildings”), the areas for which security should be ensured (hereafter, referred to as the “Controlled Areas”) shall be categorized as follows:

(1) Type I Controlled Area

Areas requiring the strictest management to which only concerned Executives and Personnel as well as concerned external persons who have been designated and authorized by the Area Control Administrators stipulated in Article 11 of the Security Regulation (Regulation #15-47) due to specific operational
requirements may have access, while all other persons are prohibited from entering.

(2) Type II Controlled Area
Areas requiring strict management to which only concerned Executives and Personnel as well as concerned external persons who have been designated and authorized by the Area Control Administrator Who is stipulated in Article 11 of the Security Regulation (Regulation #15-47) due to operational requirements may have access, while other persons are prohibited from entering.

(3) Type III Controlled Area
Areas to which only Executives and Personnel as well as persons who have received an entry permit may have access, while other persons are prohibited from entering.

Chapter 4 Management Structure for Information Security

Article 5 Information Security Chief Administrator
1. An Information Security Chief Administrator shall be assigned in the Agency.
2. The Executive Director in charge of security shall serve as the Information Security Chief Administrator.
3. The Information Security Chief Administrator shall manage operations regarding Information Security.

Article 6 Information Security Administrator
1. The Directorates and Departments shall each designate an Information Security Administrator.
2. The head of each Directorates and Departments shall serve as the Information Security Administrator.
3. The Information Security Administrator shall manage the operations related to Information Security at the Directorates and Departments to which he/she belongs.

Article 7 Information Security Assistant Administrator
1. The Directorates and Departments shall designate an Information Security Assistant Administrator under the Information Security Administrator.
2. The Information Security Assistant Administrator shall be designated by the Information Security Administrator and shall take orders from the Information Security Administrator to manage operations related to Information Security.

Article 8 Information Security Staff
1. The sections stipulated in Article 4 of the Document Management Regulation (Regulation#15-21) shall designate Information Security staff member.
2. The Document Management Staff stipulated in Article 7 of Document Management Regulation shall serve as the Information Security Staff. In addition, as necessary, the Information Security Administrator may designate additional staff members.
3. The Information Security Staff shall conduct the office work related to Information Security within the corresponding section.
Chapter 5 Management of Confidential Information

Article 9 Control/Identification/Cancellation of Confidential Information
1. The control/identification/cancellation of Top Secret Information, Secret Information, Information Limited to Authorized Staff, and Information Limited to JAXA Employees (hereafter, collectively referred to as “Confidential Information”) shall be conducted according to the following regulations.
   (1) Top Secret information is to be controlled by the Information Security Chief Administrator, who shall be responsible for granting, as well as revoking, the handling period and persons to be granted access.
   (2) Secret Information is to be controlled by Information Security Administrators or Information Security Assistant Administrators who have received orders from an Information Security Administrator and who fall under the category of department managers as stipulated in Annex Table 1 of the Approval Regulation. They shall be responsible for granting, as well as revoking, the handling period and persons to be granted access.
   (3) Information Limited to Authorized Staff is to be controlled by Information Security Administrators or Information Security Assistant Administrators who have received orders from an Information Security Administrator (hereafter, referred to as “Information Security Administrator or Assistants”). They shall be responsible for granting, as well as revoking, the handling period and persons to be granted access.
   (4) Information Limited to JAXA Employees is to be controlled by the Information Security Administrator or Assistants. They shall be responsible for granting, as well as revoking, the handling period and persons to be granted access.
2. Confidential Information for which the handling period has expired shall be regarded as information for which the designation has been cancelled, except for Confidential Information for which the handling period has been extended.

Article 10 Display of Identifications of Confidential Information, etc.
1. Top Secret Information must be identified by a label such as “TOP SECRET”.
2. Secret Information must be identified by a label such as “SECRET”.
3. Information Limited to Authorized Staff must be identified by a label such as “Information Limited to Authorized Staff”.
4. Information Limited to JAXA Employees must be identified by a label such as “Information Limited to JAXA Employees” or other identification to be defined by Information Security Administrator or Assistants.

Article 11 Management Ledger
1. The Information Security Chief Administrator shall prepare a management ledger for managing the security of Top Secret Information.
2. The Information Security Administrator or Assistants shall prepare a management ledger for managing the security of Secret Information and the Information Limited to Authorized Staff.

Article 12 Storage of Confidential Information
1. Top Secret Information shall be stored in a safe that can be locked and is placed in a Type I Controlled Area.
2. Secret information shall be stored in a Type I Controlled Area.
3. Information Limited to Authorized Staff shall be stored in a safe that can be locked and is placed in a Type II Controlled Area.
4. Information Limited to JAXA Employees shall be stored in a Type II Controlled Area.

Article 13 Reading of Confidential Information
1. The Reading of Top Secret Information shall be conducted within a Type I Controlled Area after obtaining approval from the Information Security Chief Administrator.
2. The Reading of Secret Information shall be conducted within a Type I Controlled Area after obtaining approval from the Information Security Administrator or Assistants.
3. The Reading of Information Limited to Authorized Staff and the Information Limited to JAXA Employees shall be conducted within a Type II Controlled Area.

Article 14 Copying of Confidential Information
1. Executives and Personnel may not copy Top Secret Information, except when it is specifically required in the course of operations and when a request has been approved by the President following a review by the Information Security Chief Administrator.
2. Executives and Personnel may not copy Secret Information or Information Limited to Authorized Staff, except when it is specifically required in the course of operations and when a copying request has been approved by the Information Security Administrator or Assistants.
3. Executives and Personnel may only make limited Copies of Information Limited to JAXA Employee when it is required in the course of operations.
4. If Confidential Information is Copied, it shall be treated in the same manner as its original.

Article 15 Removing of Information to a Location Outside of a Controlled Area
1. Executives and Personnel may not remove Top Secret Information from a Type I Controlled Area, except when it is specifically required in the course of operations and when a request has been approved by the President of the Agency following a review by the Information Security Chief Administrator.
2. Executives and Personnel may not remove Secret Information from a Type I Controlled Area, except when it is specifically required in the course of operations and when a request has been approved by the Information Security Administrator or Assistants.
3. Executives and Personnel may not remove Information Limited to Authorized Staff from a Type II Controlled Area, except when it is specifically required in the course of operations and when a request has been approved by the Information Security Administrator or Assistants.
4. When Removing Confidential Information, the Executives and Personnel must keep
it in their possession at all times. When removing Confidential Information through the utilization of an Information Systems, the Executives and Personnel shall utilize an Information Systems that falls under the control of Article 19-3.

Article 16 Disposal
When disposing of Confidential Information, the information must be burned, shredded, or deleted completely so that it cannot be restored.

Article 17 Lending
1. Executives and Personnel may not lend Top Secret Information to persons inside or outside of the Agency, except when it is specifically required in the course of operations and when the request has been approved by the President of the Agency following a review by the Information Security Administrator.
2. Executives and Personnel may not lend Secret Information, Information Limited to Authorized Staff, or Information Limited to JAXA Employees to persons inside or outside of the Agency, except when it is specifically required in the course of operations and when the request has been approved by the Information Security Administrator or Assistants. This regulation shall not apply to the Lending of Information Limited to JAXA Employee to Executives and Personnel.
3. When Confidential Information is Lent based on the above clause, the Confidential Information shall be returned by the designated date.

Article 18 Sending
1. Top Secret Information may not be Sent.
2. Executives and Personnel may not send Secret Information, Information Limited to Authorized Staff or Information Limited to JAXA Employee to persons inside or outside of the Agency, except for when it is specifically required in the course of operations and when the request has been approved by the Information Security Administrator or Assistants. This regulation shall not apply to the Sending of Information Limited to JAXA Employee to Executives and Personnel.

Article 18-2 Conditions and Methods for Removing, Lending, and Sending Secret Information
1. When Lending or Sending Secret Information to a person external to the Agency, as specified by Article 9-1 and 9-2, the Information Security Administrator or Assistants shall require the organizations to which the person belongs to promise to comply with the following conditions:
   (1) The recipient organization shall prepare an area that is equivalent to the Controlled Area stipulated in Article 4-1. Access to this area by persons other than the recipient person shall be controlled.
   (2) A manager shall be assigned to be responsible for handling the information, who is equivalent to the manager stipulated in Articles 5 and 6.
   (3) Recipient organization shall, as necessary, supplement its internal set of regulations to comply with the relevant provisions this Regulation and shall handle the Secret Information in accordance with those internal set of regulations.
2. The original of Secret Information and its copy made on an Information Systems shall not be removed, lent, or sent.
3. The only method allowed for lending or sending Secret Information to a recipient person/organization shall be personal hand delivery under the responsibility of the Information Security Administrator or Assistants.
4. Regardless of the stipulations contained in Items 2 and 3 above, in the case in which the Information Security Administrator recognizes that it is urgent and it will tremendously impact the smooth and proper implementation of operations, as an exceptional emergency measure, copied information which has been encrypted through the utilization of an Information Systems may be removed to a Type II Controlled Area and, using an Information Systems that complies with Article 19, lent or sent through email or other electronic transmission means.

Article 18-3 Conditions and Methods for Lending and Sending Information Limited to Authorized Staff
1. When Information Limited to Authorized Staff is lent or sent to a person who is outside of JAXA and is authorized to have access to it in accordance with Article 9-1-3, a firm commitment shall be taken from the organization to which the recipient person belongs, promising not to disclose it outside the recipient.
2. The original of Information Limited to Authorized Staff shall not be removed, lent, or sent.
3. The methods to lend or send Information Limited to Authorized Staff shall be either one of the following methods.
   (1) Means utilizing postal mail; however, the delivery must be certified postal mail and requires a delivery certificate.
   (2) Electronic transmission means such as facsimile, electronic mail, etc. In such cases the telephone number and the mailing address of the addressee of the recipient shall be well confirmed. In the case of facsimile, communication shall be made with the addressee immediately before and immediately after the facsimile is sent to confirm receipt. In the case of email, the corresponding information shall be encrypted prior to Sending it.

Article 19 Handling of Information on Information Systems
1. Information Systems on which Top Secret Information and Secret Information are transmitted shall be installed in Type I Controlled Areas and may not be recorded or stored in a network that is connected to an Information Systems outside of a Type I Controlled Area. However, if a case in question falls under Article 18-2-4, such case shall be considered to constitute an exception.
2. A sufficient level of security measures for authenticating the Executives and Personnel shall be taken with Information Systems that deal with recording, processing, and transmitting Secret Information.
3. In addition to the stipulations contained in Items 1 and 2 above, additional regulations for handling the transmission of Confidential Information by Information Systems shall be stipulated in the Information Systems Security Regulation (Regulation #15-49).
Article 20 Education and Training
1. The Information Security Chief Administrator shall prepare an annual Information Security Education and Training Plan for Executives and Personnel, and shall implement such training with the cooperation of the Directorates and Departments.
2. Executives and Personnel shall receive Information Security education and training based on the plans stated in the previous clause.

Article 21 Auditing
1. The Information Security Chief Administrator shall plan and conduct auditing regarding Information Security on an annual basis.
2. The Executives and Personnel must cooperate with the audit stated in the previous item.
3. The Information Security Chief Administrator shall take necessary measures to ensure Information Security, reflecting the audit results obtained from Item 1 above, as necessary.

Article 22 Measures Stipulated in Contracts
1. When the Agency signs a contract, the Agency shall make the corresponding contractor (including subcontractors, who shall be under the same obligations as the contractor) observe the responsibilities for ensuring security that are stipulated in the present set of regulations and other sets of security regulations which the Agency specifies, as a part of the contracting terms, and shall clarify the descriptions regarding violations of the contracted duties.
2. In the case in which the Agency signs an entrusting or other type of contract with an individual to whom the Working Regulation or Special Working Regulation do not apply, the contract must contain statements that explicitly specify as a part of the contract terms the duties for ensuring security stipulated in this set of regulations and other sets of security regulations which the Agency adopts. In addition, the stipulations that apply when the contract is violated must also be explicitly included within the contract.
3. In the case in which the Agency accepts college students, graduate students, or interns, the Agency shall apply the stipulations stated in the previous item above, restrict their access to the Tangible Assets and Information, provide education and training regarding security, and take other measures as necessary.

Article 23 Responses Taken in an Emergency with Regards to Information Security
1. As preparation for emergencies requiring urgent responses in which Information is stolen, disclosed, altered, destroyed, deleted, burned or threatened (hereafter, referred to as “Emergency”), the Information Security Administrator or Assistants shall establish an emergency management system.
2. In the case of an Emergency, the person who has discovered the corresponding Emergency shall quickly take appropriate emergency measures, and shall report the event to the Information Security Administrator or Assistants. Information Security Administrator or Assistants shall quickly undertake appropriate responses, such as executing the emergency management system, as necessary.
3. Information Security Administrator or Assistants shall report any serious Emergency
to the Information Security Chief Administrator, and undertake appropriate responses according to the directions issued by the Information Security Chief Administrator.

Article 24 Causal Analysis and Corrective Action
When a serious Emergency occurs, the Information Security Chief Administrator shall conduct an investigation of the facts and a causal analysis thereof, and take countermeasures to prevent such problem from occurring again.

Article 25 Measures for Ensuring Information Security
If the Information Security Chief Administrator recognizes it particularly necessary to ensure Information Security, he may restrict access to Confidential Information or take other necessary countermeasures.

Chapter 6: Awareness that Executives and Personnel Should Possess

Article 26 Knowledge that Executives and Personnel Should Possess
1. The Executives and Personnel must be fully aware that the information owned by the Agency contains important Information that needs to be managed carefully and strictly in order to ensure national safety and benefits, as well as international agreements.
2. The Executives and Personnel must be fully aware of the fact that managing Information appropriately is an important mission of the Agency, and must pay sufficient attention so that Information does not become disclosed through carelessness or faulty management.

Article 27 Handling Information before its Classification is Designated
When handling a piece of important Information of the Agency, even before the Information has been designated as Confidential Information, the Executives and Personnel shall strive to ensure Information Security by taking appropriate measures such as storing the Information in a safe or a drawer that can be locked or encrypting the Information. However, Top Secret Information or Secret Information must be handled at the time the Information is created, according to the stipulations contained in Articles 9-1-1 and 9-1-2.

Article 28 Disciplinary Actions, etc.
If any act occurs that violates this set of regulations, disciplinary actions shall be taken based on the Working Regulation and Special Working Regulation, according to the severity of the violation and the category of the information disclosed.

Chapter 7 Miscellaneous Provisions

Article 29 Delegated Tasks
The Information Security Chief Administrator, Information Security Administrator, or Information Security Assistant Administrator may delegate the tasks stipulated in the present set of regulations to other appropriate Executives and Personnel, with the
approval of the President of the Agency, and with the necessary items instructed.

Article 30 Exceptional Measures
In the case in which the Information Security Administrator recognizes that Secret Information or Information Limited to Authorized Staff urgently needs to be utilized, and that it will tremendously affect the smooth and appropriate implementation of operations if the procedures stipulated in the present set of regulations are conducted, the Information Security Administrator may take exceptional emergency measures such as allowing a person aside from the authorized persons to read the Information or have access to it.

Article 31 Prioritization of Security Requirements for Entrusted Operations
When the Agency is entrusted operations by an external party and the party makes requests regarding security in the contract and the President of the Agency approves such requests, security management shall be conducted based on the requests.

Article 32 Priority of Laws and Others
In case the national government reads, removes, or copies (hereinafter, “Access”) Confidential Information based on laws, government ordinances or regulations (hereafter, collectively referred to as “Laws and Others”), the Laws and Others shall have a higher priority than the present set of regulations. However, even in such a case, the government body with Access shall be informed to the effect that the corresponding Information falls under the category of Confidential Information, and shall be requested to not disclose the Information to any person other than the persons concerned, and to store the Information in a safe that can be locked in order to take necessary measures to ensure Information Security.

Article 33 Handling Special Technological Reference Materials
When handling the special technical information stipulated in the Regulation on Special Technical Information Regulation (Regulation #15-50) and or special computer programs stipulated in the Special Computer Program Regulation (Regulation #15-51), the respective regulation sets shall be followed instead of the present set of regulations.

Article 34 Detailed Provisions
Necessary items that are required to implement the present set of regulations shall be stipulated separately by notices issued by the respective Directorates and Departments.

Supplementary Provision
This set of regulations shall be enacted on October 1, 2003.

Supplementary Provision (March 29, 2004: Regulation #16-28)
This set of regulations shall be enacted on April 1, 2004.
Supplementary Provision (June 29, 2004: Regulation #16-40)
This set of regulations shall be enacted on July 1, 2004.

Supplementary Provision (May 12, 2005: Regulation #17-47)
This set of regulations shall be enacted on May 12, 2005, and applied starting on May 1, 2005.

Supplementary Provision (September 30, 2005: Regulation #17-106)
This set of regulations shall be enacted on October 1, 2005.

Supplementary Provision (March 25, 2008: Regulation #20-23)
1. This set of regulations shall be enacted on April 1, 2008.
2. In accordance to the change of Categorization of Information stipulated in Article 3(3) of this Regulation, equivalent changes required for other regulations and documents, such as President Directive, Director Directive, or Notifications defined in Article #3 to #7 in Document Formulation Regulation shall be enacted by this Regulation.