Information Systems Security Regulation

Original Regulation issued on,
October 1, 2003 as Regulation #15-49

Revised Regulation issued on,
March 29, 2004 as Regulation #16-29
November 1, 2004 as Regulation #16-56
May 12, 2005 as Regulation #17-48
September 30, 2005 as Regulation #17-105
April 4, 2007 as Regulation #19-14
August 8, 2007 as Regulation #19-63
April 22, 2008 as Regulation #120-48
February 10, 2009 as Regulation #21-2

Japan Aerospace Exploration Agency
Information Systems Security Regulation

Chapter 1 General Provision

Article 1 Purposes
The present set of regulations stipulates basic items, and thus it serves to ensure the convenience of the Information Systems owned by the Japan Aerospace Exploration Agency, an independent administrative institution, (hereafter, referred to as the “Agency”), to prevent the Information Systems owned by the Agency from being destroyed, invaded, illegally accessed, or attacked by computer viruses or other threats, and eventually to prevent the illegal uses thereof (hereafter, referred to as “Information Systems 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 Working Regulation (Regulation #15-23) and the Special Working 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. The terms “Directorates and Departments” shall refer to organizational groups such as the Directorates, Departments and others listed in Annex Table 1.
5. The term “Regional Network” shall refer to networks that constitute elements of the network of the Agency, and which is operated within each region as a unit. Specifically, it shall refer to the Tsukuba General Net, Chofu Net, Kakuta Net, and Sagamihara Net. (Hereafter, the total network of the Agency shall be referred to as the “JAXA Consolidated Network”.)
6. The term “Division” shall refer to the organizational units that manage the Information Systems and that take responsibility for operating the Information Systems.

Article 3 Ensuring Security
The executives and Personnel (hereafter, referred to as the “Executives and Personnel”) must strive to ensure security in maintaining, operating, and utilizing Information Systems owned by the Agency.

Article 4 Security Measures for Information Systems
Information Systems Security shall be ensured by taking measures according to the Information category and the risk assessment.

Article 5 Physical Security Measures for Information Systems
When maintaining, operating, and utilizing Information Systems, physical security measures such as restricting entry to the server rooms and taking countermeasures to prevent the stealing of personal computers shall be undertaken according to the Information category and the risk assessment.

Article 6 Technical Security Measures for Information Systems
When maintaining, operating, and utilizing Information Systems, technical security measures such as obtaining access records, controlling access by utilizing passwords, and taking countermeasures against computer viruses shall be undertaken according to the Information category and the risk assessment.

Article 7 (Deleted)

Chapter 2 Categorization of Information

Article 8 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 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) concerned Executives and Personnel of the Agency,
   b) concerned people of other organization than the Agency.

(4) Information limited to JAXA employee
   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 Management Structure for Information Systems Security

Article 9 JAXA Consolidated Network Administrator
1. A JAXA Consolidated Network Administrator shall be designated within the Agency.
2. The Executive Director in charge of Informatization shall serve as the JAXA Consolidated Network Administrator.
3. The JAXA Consolidated Network Administrator shall manage operations regarding Information Systems Security for the entire Agency.

Article 9-2 JAXA Consolidated Network Manager
1. A JAXA Consolidated Network Manager shall be designated within the Agency.
2. The Director of Information Systems Department shall serve as the JAXA Consolidated Network Manager.
3. The JAXA Consolidated Network Manager shall take orders from the JAXA Consolidated Network Administrator to manage operations regarding Information Systems Security for the entire Agency.

Article 10 Regional Network Administrator
1. Each of the regional networks shall have a Regional Network Administrator.
2. Persons in the positions indicated in Annexed Table 1 shall serve as Regional Network Administrators.
3. The Regional Network Administrators shall manage operations related to the security of Information Systems of the regional network over which they are responsible.

Article 11 Regional Network Manager
1. A Regional Network Manager may be designated under the Regional Network Administrators within their respective regional networks.
2. The Regional Network Manager shall be designated by the Regional Network Administrator, and shall manage operations related to Information Systems Security of the regional network over which they are responsible.

Article 11-2 Information Systems Division Administrator
1. Each Division shall designate an Information Systems Division Administrator.
2. The Information Systems Division Administrator shall manage operations related to Information Systems Security of the Information Systems that are operated and managed by the Division.

Article 11-3 Information Systems Division Manager
1. An Information Systems Division Manager may be designated under the Information Systems Division Administrator within each Division.
2. The Information Systems Division Manager shall be designated by the Information Systems Division Administrator and shall manage operations related to Information Systems Security of the Information Systems that are operated and managed by the
Division.

Article 12 Information Systems Administrator
1. Each Division shall designate an Information Systems Administrator for each of the Information Systems that the Division operates and manages.
2. The Information Systems Administrator shall take orders from the Information Systems Division Administrator to manage the corresponding Information Systems Security.

Article 12-2 Information Systems Manager
1. An Information Systems Manager may be designated under the Information Systems Administrator within each Division.
2. The Information Systems Manager shall take orders from the Information Systems Administrator to manage the corresponding Information Systems Security.

Article 13 Understanding the Maintenance and Operational Status of Information Systems
The Regional Network Administrator shall summarize the maintenance and operational status of the Information Systems on a regular basis and report the results to the JAXA Consolidated Network Administrator.

Article 14 Understanding the Information Systems Management Structure
When changes are made to the Information Systems management structure, the Regional Network Administrator shall promptly report such changes to the JAXA Consolidated Network Administrator.

Article 15 Responsibilities of Users of Information Systems
1. Executives and Personnel shall utilize the Information Systems only for the purpose of implementation of Agency operations.
2. Executives and Personnel must take appropriate Information Systems Security measures, such as appropriately managing passwords.
3. In utilizing the Information Systems, if Executives and Personnel need to connect networks, utilize wireless LANs, bring in or remove personal computers, they must obtain approval through a set of procedures separately predetermined by the Regional Network Administrator.

Article 15-2 Responsibilities of Persons who Maintain and Operate Information Systems
In maintaining and operating the Information Systems, if Executives and Personnel need to connect networks, change routing, install wireless LAN routers, transport, bring in, or remove Information Systems, or change the configuration of important systems, they must obtain approval through a set of procedures separately predetermined by the Regional Network Administrator.

Chapter 4 Education/Training, Auditing, and Emergency Responses

Article 16 Education and Training
1. The JAXA Consolidated Network Administrator shall develop Information Systems Security education and training plans for Executives and Personnel, and implement such training with the cooperation of the Directorate and Departments, on an annual basis.
2. Executives and Personnel shall receive security education and training based on the plans stated in the previous clause.
3. The Regional Network Administrator may provide education and training regarding Information Systems Security to all employees belonging to each Directorate and Department.

Article 17 Information Systems Security Auditing
1. The JAXA Consolidated Network Administrator shall plan and conduct audits regarding Information Systems Security with the cooperation of the Regional Network Administrator and Regional Network Manager (hereafter, collectively referred to as the “Regional Network Administrators/Managers”), on an annual basis.
2. The Executives and Personnel must cooperate with the auditing stated in the previous clause.
3. The JAXA Consolidated Network Administrator, with the cooperation of the Regional Network Administrators/Managers shall, as necessary, take necessary measures to ensure Information Systems Security based on the auditing results obtained from Clause 1 above.

Article 18 Responses to Information Systems Security Emergencies
1. As preparation for Information Systems Security emergencies requiring urgent responses (hereafter, referred to as “Emergency”), the Regional Network Administrators/Managers shall establish an emergency response organizational system.
2. In case of an emergency, the person who discovers the emergency shall quickly take appropriate emergency measures, and shall report the event to the Regional Network Administrator, Regional Network Manager, necessary Information Systems Division Administrator, Information Systems Division Manager, Information Systems Administrator, or Information Systems Manager (hereafter, collectively referred to as “Information Systems Administrators/Managers”).
3. When receiving the report stated in the previous clause above, the Information Systems Administrators/Managers shall cooperate with other Information Systems Administrators/Managers concerned and shall quickly undertake appropriate responses, such as executing the emergency management system, as necessary.
4. The Regional Network Administrators shall report any serious emergencies to the JAXA Consolidated Network Administrator.
5. When receiving the report stated in the previous clause above, the JAXA Consolidated Network Administrator shall take necessary measures with the respective regional networks.

Article 19 Causal Analysis and Measures
1. The Information Systems Administrators/Managers shall conduct an investigation of
the facts and a causal analysis thereof, take countermeasures to prevent such problems from occurring again and report the results of the above to the JAXA Consolidated Network Administrator.

2. When receiving reports stated in the previous clause above, the JAXA Consolidated Network Administrator shall take necessary measures with the respective regional networks.

Article 20 Measures to be Taken in order to Ensure Information Systems Security
1. Regional Network Administrators may restrict the use and suspend operation of Information Systems and take other necessary measures in order to maintain Information Systems Security.

2. The Regional Network Administrator shall report the above emergencies to the JAXA Consolidated Network Administrator.

3. When receiving the reports mentioned in the previous clause above, the JAXA Consolidated Network Administrator shall take necessary measures with the respective regional networks.

Chapter 5 Compliance of Laws and Regulations

Article 21 Laws and Regulations Regarding Information Systems Security
Executives and Personnel must observe laws regarding the prohibition of illegal access (Law #128 enacted on August 13, 1999), other laws, this set of regulations and other regulations specified by the Agency.

Chapter 6 Investigation of Prohibited Acts and Measures taken with regards to such Acts

Article 22 Prohibited Acts
1. Executives and Personnel shall not conduct the following acts when maintaining, operating or utilizing Information Systems.
   (1) Conducting illegal access or other illegal acts prohibited by law regarding the prohibition of illegal access (Law #128 enacted on August 13, 1999).
   (2) Damaging Information Systems Security by changing Information Systems configurations through which Information System security may be impeded, setting inappropriate passwords or obstructing normal operation of Information Systems.
   (3) Disclosing secrets or personal information, that has come to be known in the course of operations through the utilization of Information Systems, to others.
   (4) Damaging the reputation of the Agency, harming the interests of the Agency or disgracing personnel of the Agency through the utilization of Information Systems.
   (5) Conducting acts against the public order and morals, such as accessing inappropriate sites.
   (6) Utilizing the Information Systems for private purposes such as for purchasing or selling stocks or for mail order through the Internet, etc.
   (7) The use of Information Systems which the JAXA Consolidated Network Manager separately identifies, such as Information Systems that are privately
owned by Executives and Personnel and personal computers that are installed in public locations and utilized by unidentified multiple persons (hereinafter referred to as “Private Information Systems), is prohibited. Moreover, information that has come to be known in the course of operations (excluding public information) must not be transmitted on Private Information Systems. Furthermore, the “Information Systems” in this clause shall refer to personal computers, servers, work stations, USB memory, and other external memory devices, notwithstanding Article 2 Clause 3 above.

2. Moreover, the staff who are in charge of maintaining and operating Information Systems shall not read or disclose to others personal information that has come to be known in the course of operations, or to utilize such information for illegal purposes.

Article 23 Investigation of Prohibited Acts

1. The staffs who are in charge of maintaining and operating Information Systems shall inspect the Information Systems as necessary. If it is suspected that Personnel may have conducted any of the prohibited acts stipulated in the previous clause, they shall report such to the Regional Network Administrator. The Regional Network Administrator shall provide notification of this fact to the head of the organization to which the corresponding Personnel belong.

2. If it is suspected that the subordinate staff might have conducted any of the prohibited acts stipulated in the previous Article, the head of the organization to which the suspected Personnel belongs shall cooperate with the Regional Network Administrator to investigate the issue.

3. If the result of the investigation shows that there is a valid reason to believe that the suspected Personnel did conduct the prohibited act in question, the corresponding Personnel shall be questioned by the head of the organization.

Article 24 Disciplinary Actions, etc.

If there is any act that has violated this set of regulations, disciplinary actions shall be taken based on the Working Regulation and the Special Working Regulation, according to the degree of the violation.

Chapter 7 Matters Concerning Contracts

Article 25 Measures to be Stipulated in contracts

1. When the Agency signs a contract, the Agency shall make the corresponding contractor (including all 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.

Chapter 8 Prioritization of Requests for Security Requirements for Entrusted Operations

Article 26 Prioritization of Security Requirements for Entrusted Operations

When the Agency is entrusted work 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.

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

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

Supplementary Provision (November 1, 2004: Regulation #16-56)
This set of regulations shall be enacted on November 1, 2004.

Supplementary Provision (May 12, 2005: Regulation #17-48)
This set of regulations shall be enacted on May 12, 2005, and applied starting on May 1, 2005.

Supplementary Provision (September 30, 2005: Regulation #17-107)
This set of regulations shall be enacted on October 1, 2005.

Supplementary Provision (April 4, 2007: Regulation #19-14)
This set of regulations shall be enacted on April 4, 2007, and applied starting on April 1, 2007.

Supplementary Provision (August 8, 2007: Regulation #19-63)
This set of regulations shall be enacted on August 8, 2007, and applied starting on August 1, 2007.

Supplementary Provision (April 22, 2008: Regulation #20-48)
This set of regulations shall be enacted on April 22, 2008, and applied starting on April 1, 2008.

Supplementary Provision (February 10, 2009: Regulation #20-2)
This set of regulations shall be enacted on February 10, 2009.
Annexed Table 1

<table>
<thead>
<tr>
<th>Regional network name</th>
<th>(Regional Network Administrator)</th>
</tr>
</thead>
</table>
| Tsukuba Consolidated Net | Director  
Information Systems Department |
| Chofu Net              | Director  
Numerical Analysis Group  
Disciplinary Engineering  
Aerospace Research and Development  
Directorate |
| Kakuda Net             | Director  
Kakuda Space Center  
Space Transportation Mission Directorate |
| Sagamihara Net         | Director  
Center for Science Satellite Operation and  
Data Archive  
Institute of Space and Astronautical Science |