Security Regulation

Original Regulation issued on,

October 1, 2003 as Regulation #15-47

Revised Regulation issued on,

March 29, 2004 as Regulation #16-27
June 29, 2004 as Regulation #16-39
November 1, 2004 as Regulation #16-55
May 12, 2005 as Regulation #17-46
July 19, 2005 as Regulation #17-69
September 30, 2005 as Regulation #17-105
April 25, 2006 as Regulation #18-28
April 4, 2007 as Regulation #19-13
August 8, 2007 as Regulation #19-62
March 25, 2008 as Regulation #20-25
October 20, 2009 as Regulation #21-43

Japan Aerospace Exploration Agency
Security Regulation

Chapter 1 General Provision

Article 1 Purposes

The present set of regulations stipulates basic items, and thus it serves to maintain order in areas controlled by the Japan Aerospace Exploration Agency, an independent administrative institution (hereafter, referred to as the “Agency”), to carry out operations appropriately and smoothly, to protect rockets, satellites, aircraft, facilities and other important assets and information, for the purpose of ensuring the security of the Agency.

Article 2 Definition

In the present set of regulations, the terms listed below shall be respectively 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 and 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 Consolidated 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 “Divisions” shall refer to the organizational units that manage the Information Systems and that takes responsibility for operating the Information Systems.

Article 3 General Principles

1. The executives and Personnel (hereafter, collectively referred to as the “Executives and Personnel”) shall strive to ensure security.
2. The required standards of operations related to security shall be ensured in a comprehensive, systematic, and continuous manner.
3. Operations related to security shall be implemented quickly and appropriately according to existing conditions and circumstances.
4. When security is severely violated or compromised, such problems shall be resolved as soon as possible by utilizing the full resources of the Agency and by requesting the cooperation of related agencies.
Chapter 2 Basic Regulations for Security Management

Article 4 Target of Security
The Agency shall ensure security by protecting such important items as listed below; the confidentiality, integrity, and availability of which should be protected from intentional illegal acts or other threats. Thereby the Agency is able to implement its operations smoothly.

1. Information and Information Systems
2. All Tangible Assets that the Agency owns, such as rockets, satellites and aircraft; facilities required to operate the above; and devices and materials that constitute the above (hereafter, referred to as “Tangible Assets”).
3. Launching rockets, tracking and controlling satellites, operating aircraft, and other operations

Article 5 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 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.
Article 6 Categorization of Tangible Assets
1. In order to effectively ensure the security of Tangible Assets that the Agency retains, the Tangible Assets for which security should be ensured shall be categorized as follows:
   (1) AA
   Tangible Assets for which access is granted to only concerned Executives and Personnel as well as concerned external persons who have been designated and authorized due to operational requirements.
   (2) A
   Tangible Assets for which access is granted to only Executives and Personnel as well as concerned external persons who have been designated and authorized due to the operational requirements.
2. Tangible Assets that fall into the above-stated Tangible Assets categories shall be as described in the table below:

<table>
<thead>
<tr>
<th>Category</th>
<th>Applicable Tangible Assets</th>
</tr>
</thead>
</table>
| AA       | * Tangible Asset that includes technologies categorized as “Top Secret Information” or “Secret Information.”  
          | * Tangible Assets that if lost or damaged, would have a fatal effect on achieving the mission of the Agency, or would tremendously damage the social reputation of the Agency. |
| A        | * Tangible Assets that include technologies categorized as “Information limited to authorized staff” or “Information limited to JAXA employees.”  
          | * Tangible Assets that if lost or damaged, would have a great effect on achieving the mission of the Agency, or would damage the social reputation of the Agency. |

Article 7 Categorization of Operations
Operations conducted by the Agency, the security of which should be ensured, shall be categorized as follows according to their degree of importance and risk assessment.
   (1) AA
   Among the operations of launching rockets, tracking and controlling satellites, operating aircraft, and developing rockets/satellites/aircraft, operations that if impeded would have a fatal effect on achieving the mission of the Agency.
   (2) A
   Among operations excluding the operations stated above, operations that if impeded would have an effect on achieving the mission of the Agency.

Chapter 3 Management Organization

Article 8 Security Board
1. In order to coordinate important and common issues related to security, a Security Board (hereafter, referred to as the “Board”) shall be formed.
2. The members of the Board shall be as stated in Annex Table 2.
3. The Executive Director in charge of security shall serve as the chairman of the Board. The chairman shall represent the Board and shall manage the Board's operations.

4. As necessary, the Board may add Executives and Personnel or external experts whom the chairman specifies, in addition to the Executives and Personnel stipulated in Item 2, to the members constituting the Board.

5. As necessary, the Board may contract with external organizations to conduct investigations regarding specialized issues.

6. The Board shall set up a special committee that shall serve to coordinate important and common issues related to security (hereafter, referred to as the “Information Systems Security Committee”).

7. The members of the Information Systems Security Committee shall be as stated in Annex Table 3.

8. The chairman of the Information Systems Security Committee shall be the Executive Director in charge of Informatization. If the Board needs to meet when the Executive Director is absent, a person who has been designated by the Executive Director shall be the substitute for the chairman.

9. As necessary, the Board may add Executives and Personnel whom the chairman specifies, in addition to the Executives and Personnel stipulated in Item 7, to the members constituting the Board.

10. The Board may set up special committees that shall serve to coordinate specialized issues other than Information Systems security.

11. The chairman shall report to the President critical issues that have been coordinated or reported at the Board.

12. Operations related to the management of the Board (excluding operations related to the Information Systems Security Committee) shall be conducted by the Security Administration Office, and operations related to the management of the Information Systems Security Committee shall be conducted by the Information Systems department.

Article 9 Security Chief Administrator
1. In order to integrate all of the operations regarding security as well as to develop strategies for issues requiring Agency-wide responses, a Security Chief Administrator shall be assigned.

2. The Security Chief Administrator shall be the Executive Director in charge of security.

3. In the absence or disability of the Security Chief Administrator, the Executive Director in charge of informatization shall be the substitute.

4. The Security Chief Administrator shall bring up critical issues to the Board described above.

Chapter 4 Controlled Areas

Article 10 Categories of Controlled Areas
1. 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 Administrator 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 due to operational requirements may have access, while all 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.

2. The security of Information, Tangible Assets, and operations shall be ensured by the above-stated categorization of Controlled Areas and as shown in the table below.

<table>
<thead>
<tr>
<th>Controlled Area</th>
<th>Information, Tangible Assets, and operations to be secured</th>
</tr>
</thead>
</table>
| Type I Controlled Area | * Information categorized as “Top Secret Information” or “Secret Information”  
* Tangible Assets categorized as “AA”  
* Operations categorized as “AA” |
| Type II Controlled Area | * Information categorized as “Information Limited to Authorized Staff” or “Information Limited to JAXA Employees”  
* Tangible Assets categorized as “A”  
* Operations categorized as “A” |

Article 11 Area Control Administrator and Area Control Operations Manager

1. The Security Chief Administrator shall have Area Control Administrators; the persons shown in Annex Table 4 shall be designated as the Area Control Administrators.

2. The Area Control Administrator shall prevent acts from being conducted within Corporate Buildings that interfere with the Agency’s duties and shall manage operations related to security of the Controlled Areas.

3. The Area Control Administrator shall be authorized to designate Area Control Operations Managers who shall be in charge of ensuring the security of the respective Type I and Type II Controlled Areas stipulated in Article 10.

4. The Area Control Administrator shall designate two or more deputies, with their relative order identified.

Article 12 Responsibilities of the Area Control Administrator

1. The Area Control Administrator shall take necessary measures according to the
categories of Controlled Areas to maintain security walls and monitoring devices, manage the keys and ID card locks, use guards for monitoring and restrict entry to certain areas.

2. In order to maintain order and ensure the security of Controlled Area, as necessary the Area Control Administrator shall prohibit entry to the Controlled Area, take other such measures as may be necessary.

Article 13 Prevention of Acts that Interfere with the Agency’s Duties within Corporate Buildings

1. In order to maintain the order and safety of headquarters and the corporate branch buildings, as well as to smoothly implement the Agency’s operations, the Area Control Administrator shall not allow any act that interferes with the Agency’s duties, as exemplified by allowing hazardous materials to be brought into Corporate Buildings, unauthorized third parties to enter Corporate Buildings, any persons to destroy, damage or contaminate Corporate Buildings, or any person to force a meeting with, conduct violent behavior towards, or threaten the Executives and Personnel. However, if the Area Control Administrator recognizes that acts in question are necessary and appropriate, and that safety management measures and security management measures have been ensured, as well as if the Area Control Administrator specifies the range, method, and conditions of the acts in question and that the acts are being conducted based on his/her authorization, the above-stated restrictions shall not apply.

2. When any act that interferes with the Agency’s duties takes place, the Area Control Administrator shall take necessary measures, as exemplified by ordering the person conducting the corresponding act to leave the Corporate Buildings, stopping the corresponding act, or removing the hazardous material.

Article 14 Causal Analysis, etc.

1. In such case as described in Item 2 above, the Area Control Administrator shall conduct an investigation regarding the cause of such case, determine and take actions to eliminate recurrence, according to the degree of importance of the corresponding act that has interfered with the Agency’s duties.

2. The Area Control Administrator shall report the measures taken as stated above to the Security Chief Administrator.

3. The Security Chief Administrator shall direct the respective Area Control Administrators to take countermeasures to prevent similar incidents as required.

Chapter 5 Security of Information and Information Systems

Section 1 Structure for managing Information and Information Systems

Article 15 Information Security Chief Administrator

1. The Information Security Chief Administrator shall be under the Security Chief Administrator.

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. However, security management of Information at storage locations within the Controlled Areas shall fall under the responsibility of the respective Area Control Administrators stipulated in Article 11.

Article 16 JAXA Consolidated Network Administrator
1. A JAXA Consolidated Network Administrator shall be designated under the Security Chief Administrator.
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 for security of the Information Systems for the entire Agency.

Article 16-2 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 in an integrated manner operations regarding Information Systems security for the entire Agency.

Article 17 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 18 Information Security Assistant Administrator
1. Directorates and Departments shall designate an Information Security Assistant Manager under the Information Security Administrator.
2. The Information Security Assistant Manager 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 19 Information Security Staff
1. The sections stipulated in Article 4 of the Document Management Regulation (Regulation#15-21) shall designate Information Security Staff.
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.

Article 20 Regional Network Administrator
1. Each of the Regional Networks shall have a Regional Network Administrator.
2. The directors listed in Annexed Table 5 shall serve as the Regional Network Administrators.
3. The Regional Network Administrators shall manage operations related to the security of the Information Systems of the Regional Network over which they are responsible.

Article 20-2 Regional Network Manager
1. A Regional Network Manager may be designated under the Regional Network Administrator within their respective Regional Networks.
2. The Regional Network Manager shall be designated by the Regional Network Administrator and shall manage operations related to the Information Systems security of the Regional Network over which they are responsible.

Article 20-3 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 which are operated and managed by the Division.

Article 20-4 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 the Information Systems security of the Information Systems that are operated and managed by the Division.

Article 20-5 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 System Administrator shall take orders from the Information Systems Division Administrator to manage the corresponding Information Systems security.

Article 20-6 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 System Administrator to manage the corresponding Information Systems security.

Section 2 Information Security Measures

Article 21 Information Security Measures
Information security shall be ensured by the following measures according to the degree of importance and risk assessment of the corresponding piece of Information:
restrictions by the Information Security Administrator regarding the removal of security Information from Controlled Areas, restrictions on making copies of such Information, preparation of Information management ledgers, disposing of such Information by burning or shredding and taking appropriate measures for managing Information security. The Area Control Administrator shall implement the security measures in each of the Controlled Areas.

Article 22 Designation of Information
1. The Information Security Chief Administrator shall designate Top Secret Information based on the categorizations stipulated in Article 5.
2. The Information Security Administrators or Information Security Assistant Administrators who have received orders from the Information Security Administrator and who have been entrusted to take over the related office work and who fall under the category of director as stipulated in Annex Table 1 of the Approval Regulation, shall designate Secret Information based on the categorizations stipulated in Article 5.
3. The Information Security Administrators or the Information Security Assistant Administrators who have received orders from the Information Security Administrator and who have been entrusted to take over the related office works, shall designate Information Limited to Authorized Staff as well as Information Limited to JAXA Employees, based on the categorizations stipulated in Article 5.
4. Information that has been categorized based on the statements contained in Item 3 above shall be stored in the corresponding Controlled Areas according to the categorizations stipulated in Article 10.

Article 23 Limitations of Persons Concerned
1. In managing Information, restrictions on concerned persons shall be made clear and this scope must be restricted to the minimum degree possible.
2. Concerned persons shall be specified by the Information Security Chief Administrator with regards to Top Secret Information; and by the Information Security Administrator with regards to Secret Information and Information Limited to Authorized Staff.

Article 24 Detailed Regulations related to Information Security
In addition to the present set of regulations, the details necessary to ensure Information security shall be stipulated by the Information Security Regulation (Regulation #15-48) and other sets of regulations.

Section 3 Information Systems Security Measures

Article 25 Information Systems Security Measures
Information Systems security shall be ensured by both the security management measures defined by the Information Systems Division Administrator and the Controlled Area security measures defined by Area Control Administrator according to predefined procedures by the Regional Network Administrators based on the degree of importance and risk assessment for the Information which is stored in the
Article 26 Detailed Regulations related to Information Systems Security

In addition to the present set of regulations, the details necessary to ensure Information Systems security shall be stipulated by the Information Systems Security Regulation (Regulation #15-49) and other sets of regulations.

Chapter 6 Tangible Asset Security

Article 27 Tangible Asset Security Measures

1. The heads of Directorates and Departments shall designate the Tangible Assets according to the categories stipulated in Article 6, and shall store the Tangible Assets in Controlled Areas according to the resulting category.

2. Tangible Asset security shall be ensured by appropriate management measures taken for the Tangible Assets based on the asset management regulations, as well as security measures implemented by the Area Control Administrator for the corresponding Controlled Areas.

Chapter 7 Operations Security

Article 28 Operations Security Measures

The heads of Directorates and Departments shall designate operations based on the categories stipulated in Article 7 with regards to the operations conducted within the corresponding Controlled Area, and shall specify the Controlled Area according to the category.

Chapter 8 Miscellaneous Rules

Article 29 Education and Training

The Security Chief Administrator shall provide educational training regarding security management to Executives and Personnel periodically, as well as on an as needed basis. Note that Education and training regarding Information security management shall be provided by the Information Security Chief Administrator, and that Education and training regarding Information Systems security management shall be provided by the JAXA Consolidated Network Administrators, under their own responsibilities.

Article 30 Auditing

1. The Security Chief Administrator shall conduct regular audits regarding security management as well as on an as needed basis. However, auditing regarding Information security management shall be conducted by the Information Security Chief Administrator and auditing regarding Information Systems security management shall be provided by the JAXA Consolidated Network Administrator, under their respective responsibilities.

2. The Security Chief Administrator, Information Security Chief Administrator, and the JAXA Consolidated Network Administrator shall take necessary measures for
ensuring security, based on the auditing results, as needs arise.

Article 31 Ensuring Security outside of Controlled Areas
In cases in which tests, experiments, or the transportation of important supplies are conducted, or Information or Tangible Assets are retained outside of the Controlled Areas that the Agency specifies, the heads of Directorates and Departments that are in charge of the corresponding operations, Information, or Tangible Assets shall strive to ensure a security level that is equivalent to the security level of the Controlled Areas according to the category of the above-stated items.

Article 32 Measures 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.

Article 33 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 34 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.

Article 35 Responses taken in an Emergency
1. In cases in which accidents or disasters occur, an emergency management system must be established and necessary measures must be taken according to the stipulations regarding emergency management.
2. In advance of emergencies the President shall designate staff members to be in charge of responding to emergencies and in making preparations for the specific emergency cases listed below.
(1) Earthquakes in which normal operations can not be performed, floods, other natural disasters of a large scale, accidents of a large scale, and other man-made disasters

(2) Serious impairments that might cost lives of Executives and Personnel

3. The staff members who have been designated as stated above shall receive necessary education and training. When an emergency occurs, the staff members shall take necessary measures as quickly as possible, until an emergency management system has been established.

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

Supplementary Provision (March 29, 2004: Regulation #16-27) This set of regulations shall be enacted on April 1, 2004.

Supplementary Provision (June 29, 2004: Regulation #16-39) This set of regulations shall be enacted on July 1, 2004.

Supplementary Provision (November 1, 2004: Regulation #16-55) This set of regulations shall be enacted on November 1, 2004.

Supplementary Provision (May 12, 2005: Regulation #17-46) This set of regulations shall be enacted on May 12, 2005, and applied starting on May 1, 2005.

Supplementary Provision (July 19, 2005: Regulation #17-69) This set of regulations shall be enacted on July 19, 2005, and applied starting on July 1, 2005.

Supplementary Provision (September 30, 2005: Regulation #17-105) This set of regulations shall be enacted on October 1, 2005.

Supplementary Provision (April 25, 2006: Regulation #18-28) This set of regulations shall be enacted on May 1, 2006.

Supplementary Provision (April 4, 2007: Regulation #19-13) This set of regulations shall be enacted on April 4, 2007, and applied starting on April 1, 2007.

Supplementary Provision (August 8, 2007: Regulation #19-62) This set of regulations shall be enacted on August 8, 2007, and applied starting on August 1, 2007.

Supplementary Provision (March 25, 2008: Regulation #20-25) This set of regulations shall be enacted on April 1, 2008.
Supplementary Provision (March 25, 2008: Regulation #21-43)
This set of regulations shall be enacted on November 2, 2009.
Annex Table 1

Strategic Planning and Management Department
Industrial Collaboration and Coordination Center
Public Affairs Department
Assessment and Audit Office
General Affairs Department
Human Resources Department
Finance Department
Contract Department
International Relations Department
Security Administration Office
Tsukuba Space Center Administration Department
Chofu Aerospace Center Administration Department
Sagamihara Campus Administration Department
Space Transportation Mission Directorate
Space Applications Mission Directorate
Human Space Systems and Utilization Mission Directorate
Aerospace Research and Development Directorate
Institute of Space and Astronautical Science (ISAS)
Aviation Program Group (APG)
Lunar and Planetary Exploration Program Group
Systems Engineering Office
JAXA’s Engineering Digital Innovation Center
Safety and Mission Assurance Department
Information Systems Department
Ground Facilities Department
Spectrum Management Office
Consolidated Space Tracking and Data Acquisition Department
Environmental Test Technology Center
Space Education Office
Promotion Office for Collaboration with Universities and Research Institutes
Information Gathering Satellite Systems Development Group
Annex Table 2

Executive Director in charge of Security
Executive Director in charge of Informatization
Director of Security Administration Office
Executive Director of Space Transportation Mission Directorate or its assignee
Executive Director of Space Applications Mission Directorate or its assignee
Executive Director of Human Space Systems and Utilization Mission Directorate or its assignee
Executive Director of Aerospace Research and Development Directorate or its assignee
Executive Director of Institute of Space and Astronautical Science (ISAS) or its assignee
Program Director of Aviation Program Group (APG) or its assignee
Program Director of Lunar and Planetary Exploration Program Group or its assignee
Annex Table 3

<table>
<thead>
<tr>
<th>Position / Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Director in charge of Informatization</td>
</tr>
<tr>
<td>Senior Chief Officer of Informatization</td>
</tr>
<tr>
<td>Director of Security Administration Office</td>
</tr>
<tr>
<td>Executive Director of Space Transportation Mission Directorate or its assignee</td>
</tr>
<tr>
<td>Executive Director of Space Applications Mission Directorate or its assignee</td>
</tr>
<tr>
<td>Executive Director of Human Space Systems and Utilization Mission Directorate or its assignee</td>
</tr>
<tr>
<td>Executive Director of Aerospace Research and Development Directorate or its assignee</td>
</tr>
<tr>
<td>Executive Director of Institute of Space and Astronautical Science (ISAS) or its assignee</td>
</tr>
<tr>
<td>Program Director of Aviation Program Group (APG) or its assignee</td>
</tr>
<tr>
<td>Program Director of Lunar and Planetary Exploration Program Group or its assignee</td>
</tr>
<tr>
<td>Director of Information Systems Department or Information Systems Department</td>
</tr>
</tbody>
</table>
## Annex Table 4

<table>
<thead>
<tr>
<th>Branch Name</th>
<th>Area Control Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chofu Aerospace Center</td>
<td>Director of Chofu Aerospace Center</td>
</tr>
<tr>
<td>General Affairs Department</td>
<td>Director of General Affairs Department</td>
</tr>
<tr>
<td>Tsukuba Space Center</td>
<td>Director of Tsukuba Space Center</td>
</tr>
<tr>
<td>Sagamihara Campus</td>
<td>Director of Sagamihara Campus</td>
</tr>
<tr>
<td>Nagoya Office,</td>
<td>Director of Tsukuba Space Center</td>
</tr>
<tr>
<td>Space Transportation Mission Directorate</td>
<td>Director of Chofu Aerospace Center</td>
</tr>
<tr>
<td>Masuda Tracking and</td>
<td>Director of Masuda Tracking and Communication Station,</td>
</tr>
<tr>
<td>Communication Station,</td>
<td>Space Transportation Mission Directorate</td>
</tr>
<tr>
<td>Ogasawara Tracking Station,</td>
<td></td>
</tr>
<tr>
<td>Uchinoura Space Center</td>
<td>Director of Uchinoura Space Center</td>
</tr>
<tr>
<td>Kakuda Space Center</td>
<td>Director of Kakuda Space Center</td>
</tr>
<tr>
<td>Noshiro Testing Center</td>
<td>Manager of Noshiro Testing Center</td>
</tr>
<tr>
<td>Katsuura Tracking and</td>
<td>Director of Katsuura Tracking and Communication Station</td>
</tr>
<tr>
<td>Communication Station</td>
<td>Space Transportation Mission Directorate</td>
</tr>
<tr>
<td>Okinawa Tracking and</td>
<td>Director of Okinawa Tracking and Communication Station</td>
</tr>
<tr>
<td>Communication Station</td>
<td>Consolidated Space Tracking &amp; Data Acquisition Department</td>
</tr>
<tr>
<td>Usuda Deep Space Center</td>
<td>Director of Usuda Deep Space Center</td>
</tr>
<tr>
<td>Space Applications Mission</td>
<td>Director of Earth Observation Center (EOC)</td>
</tr>
<tr>
<td>Directorate</td>
<td>Earth Observation Center (EOC)</td>
</tr>
<tr>
<td>Office</td>
<td>Title</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>JAXA Washington D.C. Office</td>
<td>Director of JAXA Washington D.C. Office</td>
</tr>
<tr>
<td>JAXA Paris Office</td>
<td>Director of JAXA Paris Office</td>
</tr>
<tr>
<td>JAXA Bangkok Office</td>
<td>Director of JAXA Bangkok Office</td>
</tr>
<tr>
<td>JAXA Houston Office</td>
<td>Director of JAXA Houston Office</td>
</tr>
<tr>
<td>JAXA Kennedy Space Center</td>
<td>Director of JAXA Kennedy Space Center</td>
</tr>
<tr>
<td>Liaison Office</td>
<td>Liaison Office</td>
</tr>
<tr>
<td>Otemachi Branch Office</td>
<td>Director of Satellite Application and Promotion Center</td>
</tr>
<tr>
<td></td>
<td>Space Applications Mission Directorate</td>
</tr>
<tr>
<td>Airport Branch Office,</td>
<td>manager of Chofu Aerospace Center</td>
</tr>
<tr>
<td></td>
<td>Chofu Aerospace Center</td>
</tr>
<tr>
<td>Yokohama superintendent Branch</td>
<td>Manager of Safety and Mission Assurance Department</td>
</tr>
<tr>
<td>Office</td>
<td></td>
</tr>
<tr>
<td>Kansai Satellite Office</td>
<td>Manager of Industrial Collaboration &amp; Coordination Center</td>
</tr>
<tr>
<td>Regional Network</td>
<td>Regional Network Administrator</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Tsukuba Consolidated Net</td>
<td>Director of Information Systems Department</td>
</tr>
<tr>
<td>Chofu Net</td>
<td>Director of Numerical Analysis Group</td>
</tr>
<tr>
<td></td>
<td>Aerospace Research and Development Directorate</td>
</tr>
<tr>
<td>Kakuda Net</td>
<td>Director of Kakuda Space Center</td>
</tr>
<tr>
<td></td>
<td>Space Transportation Mission Directorate</td>
</tr>
<tr>
<td>Sagamihara Net</td>
<td>Director of Center for Science Satellite Operation and Data Archive Institute of Space and Astronautical Science (ISAS)</td>
</tr>
</tbody>
</table>