4.1. Security Regulation

Original Regulation issued on,

October 1, 2003 as Regulation #15-47

Amended 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
April 14, 2010 as Regulation #22-32
November 30, 2011 as Regulation #23-53

Japan Aerospace Exploration Agency
Table of Contents

Chapter 1 General Provision (Article 1 to Article 5)
Chapter 2 Implementation Structure
Section 1 Administrative Structure (Article 6 to Article 11)
Section 2 Control Structure (Article 12 to Article 20)
Chapter 3 Information Security
Section 1 General Provisions on Information Security (Article 21 to Article 27)
Section 2 "AA" Information (Article 28 to Article 39)
Section 3 "A" Information (Article 40 to Article 52)
Section 4 "B" Information (Article 53 to Article 64)
Section 5 Personal Information
Subsection 1 Personal Information General Provisions (Article 65 to Article 68)
Subsection 2 Management of Personal Information (Article 69 to Article 72)
Chapter 4 Information Systems Security
Section 1 Information Systems Security Management (Article 73 to Article 75)
Section 2 Information Systems Utilization (Article 76 to Article 78)
Chapter 5 Security of Assets
Section 1 General Provisions of Security of Assets (Article 79 to Article 80)
Section 2 "AA" Assets (Article 81 to Article 84)
Section 3 Registration to "A" Assets (Article 85 to Article 88)
Chapter 6 Security of Duties (Article 89 to Article 90)
Chapter 7 Area Security
Section 1 General Provisions of Area Security (Article 91 to Article 95)
Section 2 Type I Controlled Area (Article 96 to Article 98)
Section 3 Type II Controlled Area (Article 99 to Article 100)
Section 4 Type III Controlled Area (Article 101 to Article 103)
Chapter 8 Security Education (Article 104)
Chapter 9 Security Auditing (Article 105 to Article 107)
Chapter 10 Security Measures Under Contract (Article 108 to Article 109)
Chapter 11 Responses to Security Cases (Article 110 to Article 112)
Chapter 12 Miscellaneous Provisions (Article 113 to Article 116)
Security Regulation

Chapter 1 General Provision

Article 1 Purpose
The present regulation stipulates basic items, and thus it serves to maintain order in areas controlled by the Japan Aerospace Exploration Agency, an independent administrative institution (hereinafter referred to as "JAXA"), 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 JAXA.

Article 2 Scope
1. Assurance of the security of JAXA shall be in accordance with this regulation and other regulations provided for separately.
2. In cases where JAXA executes commissioned business and is provided with any security requirement based on the commissioned contract, and the President of JAXA finds the requirement as being appropriate, JAXA shall be in accordance with the said requirement notwithstanding this security regulation.

Article 3 Definitions
1. In this regulation, the terms listed below shall be respectively defined as follows:
   (1) "Personnel" shall refer to persons to whom the Working Regulation (Regulation #15-23) and the Special Working Regulation (Regulation #15-24) apply.
   (2) "Documents" shall refer to documents, writings, and electromagnetic records (means to records made by any electronic form, magnetic form, or any other forms not recognizable to human perception; the same shall apply hereinafter) that have been prepared or obtained by the Executives and Personnel in the course of his/her duties.
   (3) "Information" shall refer to documents, etc., created or obtained by Executives and personnel in the course of their duties, conveying knowledge or meaning about a particular matter, in the form of words, numbers and symbols.
   (4) "Personal Information" shall refer to Information about a living individual, which can identify the specific individual by name, date of birth or other description contained in such Information (including Information that can be compared with other Information and thereby identify the specific individual.)
   (5) "Retained Personal Information" shall refer to personal Information prepared or obtained by the Executives and Personnel in the course of his/her duties and is held by JAXA for its organizational use by the Executives and Personnel; however, this shall be limited to Personal Information recorded in JAXA’s documents as prescribed in Article 3, Paragraph 1, Item 2, of the Document Management Regulation (Regulation #15-21.)
   (6) "Person" shall refer to a specific individual identified by Personal
2

Article 4 General Principles
1. The Executives and Personnel shall cooperate and strive to ensure the security of JAXA.
2. The required standard 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 JAXA and requesting the cooperation of related agencies.

Article 5 Scope of Security
1. JAXA shall endeavor to ensure its security and thereby JAXA assures the smooth execution of its duties by protecting important items among the list specified below; of which confidentiality, integrity, and availability should be protected from intentional illegal acts or other threats.
   (1) Information (including Personal Information as stipulated in Article 3, Paragraph 1, Item 4)
   (2) Information Systems
   (3) Tangible assets (rockets, satellites, aircrafts, and the necessary facilities, hardware, and materials that constitute the aforementioned assets)
   (4) Duties (rocket launch, satellite tracking and control, aircraft operation, and
other operations)
(5) Areas (lands and buildings that store or handle those listed in the preceding Items which are controlled and owned by JAXA)

2. Definitions, categorization, and control methods for each preceding Item shall be in accordance with the provisions of Chapter 3 and subsequent Chapters.
Chapter 2 Implementation Structure

Section 1 Administrative Structure

Article 6 Security Board

1. In order to coordinate important and common issues related to the security of JAXA, the Security Board (hereinafter referred to as the "Board") shall be formed.

2. The Board shall consist of Executive Director for Security, Executive Director for Information, Senior Chief Officer of Information, Director of Strategic Planning and Management Department, Director of General Affairs Department, Director of Human Resources Department, Director of Security Administration Office, Director of Information Systems Department, and Directors of organization as specified in Article 7, Paragraph 1 of the Organization Regulation, or the Personnel assigned by the Directors.

3. The Executive Director for Security shall serve as the chairman of the Board. The chairman shall represent the Board and manage operation of the Board.

4. As necessary, in addition to the Executives and Personnel stipulated in Paragraph 2, the chairman may appoint other Executives and Personnel or external experts to the members constituting the Board.

5. As necessary, the Board may contract with external organizations to investigate specialized issues.

6. The Board shall organize a special committee that shall serve to coordinate important and common issues related to the security (hereinafter referred to as the "Information Systems Security Committee.")

7. The members of the Information Systems Security Committee shall consist of Executive Director for Information Systems, Senior Chief Officer of Information, Director of Security Administration Office, Director of Information Systems Department, and Directors of organization as specified in the Organization Regulation Article 7(1), or Personnel assigned by the Directors.

8. The chairman of the Information Systems Security Committee shall be the Executive Director for Information Systems. If the Board needs to be held 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, in addition to the Executives and Personnel stipulated in Paragraph 7, the chairman may appoint other Executives and Personnel to the members constituting the Board.

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

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

12. Operation 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.

13. Other matters necessary for the operation of the Committee shall be determined for separately by the Security Chief Administrator.
Article 7 Security Chief Administrator
1. In order to integrate all of operations regarding the security of JAXA, as well as to develop strategies for issues requiring organization-wide responses, the Security Chief Administrator shall be assigned.
2. The Executive Director for Security shall serve as the Security Chief Administrator.
3. In the absence or disability of the Security Chief Administrator, the Executive Director for Information Systems shall be the substitute.
4. The Security Chief Administrator shall bring up critical issues to the Board stipulated in the preceding Article.

Article 8 Security Assistant Chief Administrator
1. The Security Chief Administrator shall be assigned to JAXA.
2. The Director of Security Administration Office shall serve as the Security Assistant Chief Administrator.
3. The Security Assistant Chief Administrator shall manage and coordinate the security of JAXA other than Information Systems under the instructions of Security Chief Administrator.

Article 9 Information Systems Security Chief Administrator
1. The Information Security Chief Administrator shall be established under the Security Chief Administrator.
2. The Executive Director for Information Systems shall serve as the Information Systems Security Chief Administrator.
3. The Information Systems Security Chief Administrator shall manage organization-wide operations regarding Information Systems security.

Article 10 Deputy Information Systems Security Chief Administrator
1. The Deputy Information Security Chief Administrator shall be established under the Information Systems Security Chief Administrator.
2. The Senior Chief Officer of Information Systems shall serve as the Deputy Information Systems Security Chief Administrator.
3. The Deputy Information Systems Security Chief Administrator shall assist the Information Systems Security Chief Administrator, and under his/her instructions, shall manage and coordinate organization-wide operations regarding the Information Systems security.

Article 11 Information Systems Security Assistant Administrator
1. The Information Systems Security Assistant Administrator shall be assigned to JAXA.
2. The Director of Information Systems Department shall serve as the Information Systems Security Assistant Administrator.
3. The Information Systems Security Assistant Administrator shall manage and coordinate organization-wide operations regarding the Information Systems security under the instructions of the Information Systems Security Chief Administrator and the Deputy Information Systems Security Chief Administrator.
Section 2 Control Structure

Article 12 Security Control Administrator
1. Each Directorate and Department shall designate the Security Control Administrator.
2. The Directors of each Directorate and Department shall serve as the Security Control Administrator.
3. The Security Control Administrators shall administrate the security operations of the Directorates or the Departments to which he/she belongs.

Article 13 Security Control Assistant Administrator
1. Each Directorate and Department shall designate the Security Control Assistant Manager under the Security Control Administrator.
2. The Security Control Assistant Administrator shall be designated by the Security Control Administrator and under the instructions of the Security Control Administrator to collectively coordinate the Security related duties.
3. More than one Security Control Assistant Administrator may be designated and their each responsible scope shall be defined.

Article 14 Security Control Staff
1. The Security Control Staff shall be designated by the Security Control Assistant Administrator as defined in the preceding Article.
2. The Security Control Staff shall be designated by the Security Control Assistant Administrator and the responsible scope shall be defined.
3. The Security Control Staff shall engage in clerical work related to security within the designated scope.

Article 15 Area Control Administrator
1. The Area Control Administrators shall be designated for each facility or office, and the persons as shown below shall be designated as the Area Control Administrators.

<table>
<thead>
<tr>
<th>Name of facilities or offices</th>
<th>Designated Area Control Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters Office and Aerodrome Branch</td>
<td>Director of Chofu Aerospace Center (CAC)</td>
</tr>
<tr>
<td>Tsukuba Space Center (TKSC)</td>
<td>Director of TKSC</td>
</tr>
<tr>
<td>Sagamihara Campus</td>
<td>Director General of Institute of Space and Astronautically Science (ISAS)</td>
</tr>
<tr>
<td>Tokyo Office</td>
<td>Director of General Affairs Department</td>
</tr>
</tbody>
</table>
2. The Area Control Administrator shall manage operations regarding security of the designated controlled areas.
3. The Area Control Administrator shall designate two or more deputies, with their relative order identified.
4. 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.

5. The Security Control Administrators of each Directorate and Department, etc. shall follow directions in regard to the area security control in facilities to which the Area Control Administrators are assigned.

Article 16 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 managed and operated by the Division.

Article 17 Information Systems Division Manager
1. The 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 18 Information Systems Administrator
1. Each Division shall designate the Information Systems Administrator for each of the Information Systems that the Division operates and manages.
2. The Information Systems Administrator shall receive instructions from the Information Systems Division Administrator to administrate the Division's Information Systems security.

Article 19 Information Systems Manager
1. The Information Systems Manager may be designated under the Information Systems Administrator within each Division.
2. The Information Systems Manager shall receive instructions from the Information Systems Administrator to manage and coordinate the Division's Information Systems security.

Article 20 Change of the Managing Structure
The Security Control Administrators of each Directorate and Department shall report to the Security Chief Administrator when there is a change of the Security Control Assistant Administrator or the Security Control Staff. Security Control Administrators of each Directorate and Department shall report to the Information Systems Security Chief Administrator when there is a change of the Information Systems Division Administrator, the Information Systems Division Manager, the Information Systems Administrator, or the Information Systems Manager.
Chapter 3 Information Security

Section 1 General Provisions on Information Security

Article 21 Definitions in Handling Information
The terms listed below in this Chapter shall be defined as follows.
(1) "Reading" shall refer to searching and reading a content of Information (including searching a content of electromagnetic Information using Information Systems.)
(2) "Copying" shall refer to the duplication of Information by way of handwriting, machines such as copier, or Information Systems.
(3) "Removing" shall refer to the removal by the Executives and Personnel of a piece of Information to a location outside of the normal storage area and placing the Information under his/her own control.
(4) "Lending" shall refer to entrusting by the Executives and Personnel of a piece of Information to the concerned persons inside or outside JAXA, and placing the Information under the control of the persons for a certain period of time.
(5) "Providing" shall refer to transmitting or handing over Information to a person and placing the Information under the control of the person including its disposal.
(6) "Disposing" shall refer to erasing Information physically (deleting electromagnetically for electromagnetic data.)
(7) "Transferring" shall refer to the change of control of the original Information from one Security Control Administrator to another Security Control Administrator.

Article 22 General Principles of Information Control
1. Information owned by JAXA, the security of which must be ensured, shall be controlled based on the categorization as stipulated in Articles 24 to 26 according to the degree of importance and results of risk assessment.
2. Category of Information shall be designated by the Security Control Administrator or the Security Control Assistant Administrator who has been received instructions and delegated its clerical work by the Security Control Administrator (note that for "AA" Information management, the Security Control Administrator’s delegation to the Security Control Assistant Administrator shall be limited to the Directors of each Department or above ranks, hereinafter referred to as the Security Control Administrator, etc. as stipulated in Article 3 of the Decision-making Authority Regulation.) Designation of category shall be determined properly according to the characteristics of the Information.
3. The Security Control Administrators, etc. of each Directorate and Department, etc. shall prepare a registry for "AA" Information as stipulated in Article 24 and "A" Information as stipulated in Article 25 (hereinafter referred to as Information Requiring Protection) to register designated Information and another registry for recording the acts of Reading, Copying, Removing, Lending, Providing, and Disposing in regard to these Information.
4. Reading, Copying, Removing, Lending, Providing, Disposing, or Transferring of designated Information shall be conducted with the permission of the Security Control Administrator, etc. and the acts shall be recorded.
5. When a nation, etc. Reads, Removes, Copies, etc. (hereinafter referred to as Reading, etc.) secret Information, etc. based on laws, cabinet orders, or ordinances (hereinafter referred to as Laws or Ordinances); the corresponding Laws or Ordinances shall be followed notwithstanding the provisions of this regulation. In this case, however, responsible Executives and Personnel shall inform the nation, etc. of the Information that requires ensuring the security, as well as asking the nation, etc. to ensure appropriate control of the Information. Responsible Executives and Personnel further shall record the act of Providing the Information.

Article 23 Knowledge that Executives and Personnel Should Possess
1. Executives and Personnel must be fully aware that the Information owned by JAXA contains important Information that needs to be managed carefully and strictly in order to ensure national security and benefits, and in accordance with the international agreements.
2. Executives and Personnel must be fully aware of the fact that managing Information appropriately is an important mission of JAXA, and must pay sufficient attention so that Information does not become disclosed through carelessness or faulty management.
3. Executives and Personnel shall endeavor to keep the acquisition and holding of security Information at a minimum in order to lower the risk of Information leakage.

Article 24 "AA" Information
1. "AA" Information is information which needs to be ensured that it is known only to limited concerned internal and external persons, and the leakage, destruction, alteration, loss or damage of which may significantly damage national security and interests, or anything that makes JAXA's operation extremely difficult, which falls under any of the following criteria.
   (1) Information, from among information about the both technology and equipment which have been imported on the basis of the international agreements, which needs to be prevented from leaking to persons other than the particular concerned persons.
   (2) Information which the government has requested to handle strictly in terms of national security or information that JAXA has specified itself, in accordance with government requests.
   (3) Information pertaining to rocket technology, etc., as set forth in Paragraph 4 of the Appended Table of the Foreign Exchange Order (1980 Cabinet Order No. 260), concerning essential components, systems and construction necessary for JAXA's rockets to have specific features and capabilities.
   (4) Information from which there might be a serious risk of problems arising, due to the leakage, destruction, alteration, loss or damage, etc., and unless countermeasures are implemented, rocket, satellite and the space station development, launches and operation, etc., cannot continue.
   (5) Information similar to the preceding each Item and has been designated by the Security Control Administrator.
Article 25 "A" Information
1. "A" Information is information which falls under any of the following criteria and needs to be ensured that it is known only to limited internal and external persons, and the leakage, destruction, alteration, loss or damage of which may possibly damage JAXA's smooth operation, financial income, position as a contracting party, cooperation agreement, joint research partners' interests, and organizational and individual stakeholder's legitimate interests and rights, such as human right and privacy.
   (1) Information pertaining to the manufacture of systems and components, which are technologies listed in the Appended Table of the Foreign Exchange Order.
   (2) Information obtained from the other party of a contract or joint research partners, which requires special handling, such as limiting the disclosure to the persons other than the parties concerned.
   (3) Information relating to JAXA's technology, human resources, accounting and contracts which, if leaked, would cause significant damage to JAXA's operation and interests.
   (4) Information similar to the preceding each Item for which there might be a risk of duties being hindered due to its leakage, which unless appropriate measures are taken, would make smooth operation of the organization difficult.
2. Among the Retained Personal Information prescribed in Article 3, Paragraph 1, Item 5, Information which falls under any of the following items is referred to as "A" Personal Information.
   (1) Information relating to Executives and Personnel, as well as individuals who are involved in JAXA's operation, not known to the public, such as address, home telephone number, date of birth, etc., which cannot usually be known to persons other than the person himself/herself and particular concerned parties, as well as information related to personnel matters, salary and various allowances, etc.
   (2) Inquiries from individuals outside JAXA, questionnaire with names, records of responses to opinions and complaints (except for cases where only name and contact information are included.)
   (3) Personal Information files as defined in Article 2 of the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc. (Law No.59, 2003; Hereinafter referred to as "Personal Information Protection Act"), containing the records of 1000 or more individuals.

Article 26 "B" Information
1. "B" Information is information designated by the Security Control Administrator which is not applicable to information in need of protection, but requires a certain amount of care and procedures when handling it to accomplish JAXA's operation smoothly.
2. "B" Personal Information is the Retained Personal Information prescribed in Article 3, Paragraph 1, Item 5, which should be managed as "B" Information as stipulated in Section 5 of this Chapter and falls under any one of the followings.
   (1) Executives and Personnel's individual Information used in JAXA, such as affiliation, title, identification number, attendance management, and Information to be used in common and laterally in each Directorate and
Department, such as extension numbers, seating charts, committee members’ list, visitors' record, etc., (excluding Information that falls on "A" Personal Information.)

(2) Emergency contact network for an emergency case and telephone numbers list for contacting persons relating to duties (hereinafter referred to as "Emergency Contact Network, etc.", excluding those that fall under "A" Personal Information.)

(3) Information on business cards, such as a company and department name, name of a person in charge, as well as lists compiling such information (excluding those that fall under "A" Personal Information.)

Article 27 Operation Plan for Each Directorate and Department, etc.
Regarding the Information, the Security Control Administrator of each Directorate and Department, etc. shall set plans for managing each Directorate and Department including the guidelines of Information classification.

Section 2 Handling of "AA" Information
Article 28 Registration and Deregistration of "AA" Information
1. When the Security Control Administrator, etc. designate "AA" Information, the term which the Information is treated as "AA" Information and the authorized concerned persons who can access the said Information shall be designated and recorded on the registry.

2. The registration stated in the preceding Paragraph shall be conducted when acquiring or compiling "AA" Information. Even when the "AA" Information is in the process of compiling, the "AA" Information shall be treated as the same as the completed "AA" Information.

3. The extent of "AA" Information from the said Information shall be at the minimum.

4. Minimum necessary individuals shall be designated as the authorized concerned persons, who may access the "AA" Information. This designation shall be given to each person and not be given to groups of each Directorate and Department, etc.

5. When the term set at the designation and registration of "AA" Information expires or even in the middle of the term, in the event that the said Information does not need to be treated as "AA" Information anymore, or "AA" Information is no longer necessary and disposed, the declassification, and the cancellation of the registration shall be conducted. When the said term expires, the classification of the said Information is considered as declassified.

Article 29 Indication of "AA" Information
Documents which include "AA" Information shall be indicated on all the pages for the purpose of discrimination. Page number should be placed on all the pages of the said document in order to avoid being taken out. Information written on the electromagnetic media (hereinafter called "Electronic Information") shall be treated as same.
Article 30 Storage of "AA" Information
"AA" Information shall be stored in the locked stack room, etc. in Type I Controlled Area. Electronic Information shall be stored in the Information Systems located in Type I Controlled Area, which has no access to network.

Article 31 Reading of "AA" Information
1. Only designated concerned persons may Read "AA" Information.
2. When designated concerned persons Read the said Information, a written application shall be submitted in advance and shall be approved by the Security Control Administrator, etc. Reading shall be conducted within Type I Controlled Area. Reading of the Electronic Information shall be conducted using the Information Systems located in Type I Controlled Area, which has no access to network.
3. The fact of the Reading stipulated in the preceding Paragraph shall be recorded in the management record.

Article 32 Copying of "AA" Information
1. "AA" Information shall not be Copied unless it is particularly necessary in the course of duties.
2. When Copying the said Information, the designated concerned persons of JAXA shall request in writing and be given permission from the Security Control Administrator etc. Copying of the said Information shall be conducted in Type I Controlled Area. Copying of the Electronic Information shall be conducted using Information Systems located in Type I Controlled Area which has no access to network.
3. The fact of Copying as stipulated in the preceding Paragraph shall be recorded in the management record and registered pertaining to the copied Information on the registry.

Article 33 Removing of "AA" Information
1. The original "AA" Information shall not be Removed from the storage area except for the case of Transfer stated in Article 37. In the event that Removing is necessary for duties, designated concerned persons in JAXA may Copy and Remove the said Information.
2. When Removing the said Information, the designated concerned persons of JAXA shall request in writing and receive the permission from the Security Control Administrator, etc.
3. When Removing the "AA" Information after receiving the permission stated in the preceding Paragraph, the said Information shall be secured in a bag and carried with the permitted person by himself/herself. This also applies in the event that the Electronic Information is Removed by recording it on recording media. In addition, in the case where a copy is created for Removal (which includes Copying Electronic Information), the copy shall be conducted in accordance with "Copying of 'AA' Information" stipulated in Article 32.
4. Copy created based on the preceding provisions, shall be disposed immediately when the said copy is no longer necessary.
5. The fact of the Removal stated in the three preceding Paragraphs (including the
making and Disposing of copy) shall be recorded in the management record.

Article 34 Lending of "AA" Information
1. "AA" Information shall not be lent out from the storage area. When Lending is particularly necessary for duties, a copy of said Information shall be lent to the designated concerned persons.
2. When Lending, the designated concerned persons shall request in writing and receive the permission from the Security Control Administrator, etc. When given permission, the return due date shall be determined in advance.
3. When Lending out "AA" Information after receiving the permission stated in the preceding Paragraph, Article 33, Paragraphs 3 and 4 shall apply mutatis mutandis.
4. The fact of Lending stated in the preceding two Paragraphs and returning the said Information (including making and Disposing of copy) shall be recorded in the management record.

Article 35 Providing of "AA" Information
1. The original of "AA" Information shall not be Provided. When particularly necessary in the course of duties, the copy may be Provided with the designated concerned persons.
2. Notwithstanding the preceding Paragraph, when the Security Control Administrator recognizes that a case is in emergency situation and may hinder the smooth operation of duties, Providing of coded, Copied Information using Information Systems may be allowed, under the condition that the Information is taken out to Type II Controlled Area and sent via an e-mail or other electronic means using secured Information Systems.
3. When Providing "AA" Information, designated concerned persons shall request in writing prior to Providing and receive the permission of the Security Control Administrator, etc.
4. When Providing "AA" Information based on the permission in the preceding Paragraph, Article 33, Paragraph 3 shall apply mutatis mutandis.
5. When Providing "AA" Information based on the preceding Paragraph 3, the fact shall be recorded in the management record of the provider.
6. When Provided with "AA" Information, the Security Control Administrator, etc. of each Directorate and Department, etc. to which the provided person belongs shall register said Information in the registry and implement necessary control as "AA" Information in accordance with the registration procedure as stipulated in Article 28.

Article 36 Condition of Lending or Providing
When Lending or Providing "AA" Information to external concerned persons, the Security Control Administrator, etc. shall assure that the company, etc. to which the persons belong, implements same level of Information control system with this regulation for the lent or provided Information.

Article 37 Transfer of "AA" Information
1. The Security Control Administrator shall, when Transferring "AA" Information to another Security Control Administrator, record the transferee and expunge the
Information from his/her registry.

2. When taking "AA" Information out of the storage for the purpose of Transferring, Article 33, Paragraph 3 shall apply mutatis mutandis.

3. The Security Control Administrator, etc. who has received the Transferred Information, shall register said Information in a registry in accordance with Article 28 "Registration and deregistration of 'A' Information" and implement necessary control as "AA" Information.

Article 38 Disposal of "AA" Information
When Disposing Documents, etc. that contain "AA" Information, the concerned persons shall incinerate or physically shred or crush using a shredder or a media crusher of said Information by themselves. Electronic Information shall be in the non-recoverable condition using a wiping tool.

Article 39 Disclosure to Unauthorized Persons
1. When it becomes necessary for a person other than the designated concerned persons to borrow or request the Providing of "AA" Information, he/she shall request in writing to the Security Control Administrator, etc. who control said Information and receive his/her permission.

2. The Security Control Administrator, etc. when he/she has been requested for permission as stipulated in the preceding Paragraph 1, may permit such request after rigorously examining the purpose, reasons, and necessity. When giving the permission, the range of accessible Information shall be restricted to the minimum. In addition, the Security Control Administrator, etc. shall clearly indicate the condition that said Information requires ensured security and shall be taken same level of measures with this regulation to ensure the security.

3. The Security Control Administrator, etc. shall, when having the permitted person Read "AA" Information under the permission as stipulated in the preceding Paragraph, confirm that said Reading is conducted in accordance with Article 31 and with the attendance of concerned persons.

4. The Security Control Administrator, etc. shall, when Lending or Providing with "AA" Information to the permitted persons under the permission as stipulated in the preceding Paragraph 2, confirm that said Lending and Providing are conducted in accordance with Article 34 or Article 35 and shall have the permitted persons implement same level of security control with this regulation to which the Information is lent or provided.

Section 3 "A" Information

Article 40 Registration and Deregistration of "A" Information
1. When the Security Control Administrator, etc. designate "A" Information, the term which the Information is treated as "A" Information and the designated concerned persons who can access the said Information shall be designated and recorded on the registry.

2. Designation of "A" Information shall be limited to the extent of said "A" Information. This designation, however, may be given to a unit of folders such as Documents, document files, and Electronic Information.
3. Designation of concerned persons who may access "A" Information may be given to groups of each Directorate and Department, etc.
4. When cancelling the registration of "A" Information, Article 28, Paragraph 5 shall apply mutatis mutandis.

Article 41 Handling of "A" Information before its Designation
When handling Information that is likely to be designated as "A" Information, the said Information shall be taken appropriate measures which include storing in the locked stack room, etc. and in the drawer, etc., and encoding Information even before its designation as "A" Information.

Article 42 Indication of "A" Information
Documents which include "A" Information shall be indicated for the purpose of discrimination. Information written on the Electronic Information shall be treated as same.

Article 43 Storage of "A" Information
"A" Information shall be stored in the locked stack room, etc. in Type II Controlled Area. Electronic Information shall be stored in the access-controlled Information Systems located in Type II Controlled Area.

Article 44 Reading of "A" Information
1. Only designated concerned persons may Read "A" Information.
2. When Reading "A" Information, the said Reading shall be conducted within Type II Controlled Area. Reading of Electronic Information shall be conducted using access-controlled Information Systems located in Type II Controlled Area.

Article 45 Copying of "A" Information
1. "A" Information shall not be Copied unless it is necessary in the course of duties.
2. When Copying the said Information, the designated concerned persons of JAXA shall conduct in Type II Controlled Area under the permission from the Security Control Administrator etc. Copy of the said Information shall be conducted in the Type II Controlled Area. Copy of the Electronic Information shall be conducted using Information Systems located in Type II Controlled Area.
3. The fact of Copying as stipulated in the preceding Paragraph shall be recorded in the management record and registered pertaining to the Copied Information on the registry.

Article 46 Removing of "A" Information
1. "A" Information may be Removed by only the designated concerned persons of JAXA when it is necessary in the course of duties.
2. When Removing the said Information, the designated concerned persons of JAXA shall receive the permission from the Security Control Administrator, etc.
3. When Removing the "A" Information after receiving the permission stated in the preceding Paragraph, the said Information shall be secured in a bag and carried with the permitted person by himself/herself. This also applies in the event that
the Electronic Information is Removed by recording it on recording media. In addition, in the case where the copy is created for the Removal (which includes Copying of Electronic Information), the copy shall be conducted in accordance with "Copying of 'A' Information" stipulated in Article 45 except for the temporal use.

4. Copy created based on the preceding provision, shall be disposed immediately when the said copy is no longer necessary.

5. The fact of the Removal stated in the three preceding Paragraphs (including the making and Disposing of copy) shall be recorded in the management record.

Article 47 Lending of "A" Information
1. "A" Information may be Lent out to only the designated concerned persons of JAXA when it is necessary in the course of duties.
2. When Lending, the designated concerned persons shall receive the permission from the Security Control Administrator, etc. When given permission, the return due date shall be determined in advance.
3. When Lending out "A" Information after receiving the permission stated in the preceding Paragraph, Article 46, Paragraphs 3 and 4 shall apply mutatis mutandis.
4. The fact of Lending stated in the preceding two Paragraphs and returning the said Information (including making and Disposing of copy) shall be recorded in the management record.

Article 48 Providing of "A" Information
1. The original of "A" Information shall not be provided. When necessary in the course of duties, the copy may be Provided with only the designated concerned persons.
2. When Providing "A" Information, designated concerned persons shall receive the permission of the Security Control Administrator, etc.
3. When Providing "A" Information under the permission in the preceding Paragraph, methods listed below may be used other than handing to the permitted person. If Copying for Providing, "Copying of 'A' Information" in Article 45 shall be followed except for the temporal use.
   (1) Postal mail etc. which have the delivery tracking system.
   (2) Facsimile, e-mail, and other electronic transmission. When using these methods, the sender shall confirm the telephone number, e-mail address, etc. of the person to which the Information is provided, notify the receiver before Providing via facsimile, confirm that the receiver has received the Information immediately after Providing, and send coded Information via e-mail.
4. When Providing "A" Information based on the preceding Paragraphs 1-3, the Providing shall be recorded in the management record of the provider.
5. When a Directorate or Department, etc. is Provided with "A" Information, the Security Control Administrator, etc. of the Directorate or Department, etc. shall register said Information in the registry and implement control as "A" Information.
Article 49 Condition of Lending or Providing
When Lending or Providing "A" Information to external concerned persons, the Security Control Administrator, etc. shall assure that the company, etc. to which the persons belong, implements same level of Information control system with this regulation for the lent or provided Information.

Article 50 Transfer of "A" Information
1. The Security Control Administrator shall, when Transferring "A" Information to another Security Control Administrator, record the transferee and expunge the Information from his/her registry.
2. When taking "A" Information out of the storage for the purpose of Transferring, Article 46, Paragraph 3 shall apply.
3. The Security Control Administrator, etc. to which the Information is Transferred shall register said Information in a registry and implement necessary control as "A" Information in accordance with the registration procedure as stipulated in Article 40.

Article 51 Disposal of "A" Information
1. When Disposing Documents, etc. that contain "AA" Information, the concerned persons shall incinerate, physically shred or crush using a shredder or a media crusher of said Information by themselves. Electronic Information shall be in the non-recoverable condition using a wiping tool.
2. When outsourcing Disposal of "A" Information, any necessary measures to ensure security shall be taken, e.g. conducting dissolution processing keeping Documents packed on JAXA’s premises.

Article 52 Disclosure to Unauthorized Persons
1. When it becomes necessary for a person other than the designated concerned persons to Read, borrow or request the Providing of "A" Information, he/she shall request in writing to the Security Control Administrator, etc. who control the Information and receive his/her permission.
2. The Security Control Administrator, etc., when he/she has been requested for permission as stipulated in the preceding Paragraph 1, may permit such request after examining the purpose, reasons, and necessity. When giving the permission, the range of accessible Information shall be restricted to the minimum. In addition, the Security Control Administrator, etc. shall clearly indicate the condition that said Information requires ensured security and shall be taken same level of measures with this regulation to ensure the security.
3. The Security Control Administrator, etc., when Lending, Providing with, or having the permitted person Read "A" Information, shall follow each Article of this Section.
4. Request for "A" Information by persons listed in each of the followings, the request in writing as stipulated in the preceding Paragraph 1 may be omitted and oral request explaining the purpose, reasons, and necessity may be the substitute. In this case, recording in the management record shall not be omitted.
(1) Executives and Personnel not designated as the concerned persons
(2) Public officers, etc. who are obliged to ensure the confidentiality by Laws
or Ordinances
(3) Contractors who are obliged to ensure the confidentiality in accordance with JAXA's Basic and Standard Business Contract and to take the same level of security control system with JAXA pertaining to the handling of Information

Section 4 "B" Information

Article 53 Designation of "B" Information
1. Designation of "B" Information shall be limited to the extent of said "B" Information. This designation, however, may be given to a unit of folders such as Documents, document files, and Electronic Information.
2. The range of accessible persons to "B" Information may be limited only to the designated internal and external concerned persons.
3. The method for designating concerned persons who may access "B" Information shall be stipulated in accordance with Article 27, in the Implementation Guideline established by the Security Control Administrator of each Directorate and Department, etc.

Article 54 Handling of "B" Information before its Designation
When handling Information that is likely to be designated as "B" Information, the said Information shall be taken appropriate measures including storing in the locked stack room, etc. and encoding Information even before its designation.

Article 55 Indication of "B" Information
Documents which include "B" Information shall be indicated for the purpose of discrimination. Information written on the Electronic Information shall be treated as same.

Article 56 Storage of "B" Information
"B" Information shall be stored in the locked stack room, etc. in Type II Controlled Area. Electronic Information shall be stored in Information Systems located in Type II Controlled Area.

Article 57 Reading of "B" Information
Only designated concerned persons may Read "B" Information.

Article 58 Copying of "B" Information
"B" Information may be Copied by only the Executives, Personnel, and external concerned persons to the extent necessary to perform their duties.

Article 59 Removing of "B" Information
1. "B" Information may be Removed by only the Executives and Personnel to the extent necessary to perform their duties.
2. When Removing "B" Information, Executives and Personnel shall always pay attention not to lose or be stolen.
Article 60 Lending of "B" Information
1. "B" Information may be Lent out to the Executives, Personnel, and external concerned persons to the extent necessary to perform their duties.
2. When Lending out to the external concerned persons, the fact of Lending shall be recorded in the management record.

Article 61 Providing of "B" Information
1. "B" Information may be Provided with the Executives, Personnel, and external concerned persons to the extent necessary to perform their duties.
2. When Providing with the external concerned persons, the fact of Providing shall be recorded.

Article 62 Condition of Lending or Providing
When Lending or Providing "B" Information to external concerned persons, the Security Control Administrator, etc. shall assure that the company, etc. to which the persons belong does not disclose the Lent or Provided Information other than the said concerned persons.

Article 63 Disposal of "B" Information
When Disposing "B" Information, "Disposal of 'A' Information" in Article 51 shall apply mutatis mutandis.

Article 64 Disclosure to Unauthorized Persons
1. When it becomes necessary for a person other than the Executives, Personnel, and designated concerned persons to Read, borrow or request the Providing of "B" Information, he/she shall request in writing to the Security Control Administrator, etc. who control the Information and receive his/her permission.
2. The Security Control Administrator, etc., when he/she has been requested for permission as stipulated in the preceding Paragraph 1, may permit such request after examining the purpose, reasons, and necessity. When giving the permission, the range of accessible Information shall be restricted to the minimum. In addition, the Security Control Administrator, etc. shall clearly indicate the condition that said Information requires ensured security and shall be taken same level of measures with this regulation to ensure the security.
3. The Security Control Administrator, etc., when Lending, Providing with, or having the permitted person Read "B" Information, shall follow each Article of this Section.
4. Request for "B" Information by persons listed in each of the followings, the request in writing as stipulated in the preceding Paragraph 1 may be omitted, and oral request explaining the purpose, reasons, and necessity may be the substitute. In this case, recording in the management record shall not be omitted.
   (1) Executives and Personnel not designated as the concerned persons (if limiting accessible persons to "B" Information to only concerned persons in accordance with Article 53, Paragraph 2.)
   (2) Public officers, etc. who are obliged to ensure the confidentiality by Laws or Ordinances.
   (3) Contractors who are obliged to ensure the confidentiality in accordance
with JAXA's Basic and Standard Business Contract and to take the same level of security control system with JAXA pertaining to the handling of Information.

Section 5 Personal Information
Subsection 1 General Provisions of Personal Information

Article 65 General Provisions for Handling Personal Information
1. Executives and Personnel shall handle Retained Personal Information in accordance with the Act on Protection of Personal Information, related Laws, Ordinances, guidelines, and instructions by the Security Control Administrator.
2. Executives and Personnel shall not access Retained Personal Information for purposes other than the purpose of conducting duties, even if they are designated to access.

Article 66 Prohibition of Improper Use and Acquisition
1. Executives and Personnel shall not conduct any of the followings:
   (1) to disclose the Personal Information acquired in the course of the duty to another person without a justifiable ground.
   (2) to use the Personal Information acquired in the course of the duty for an unjustifiable purpose.
   (3) to acquire Personal Information by a deception and other wrongful means.

Article 67 Indication of the Purpose of Use
1. When Executives and Personnel directly acquire Personal Information on a Person that is recorded in a document (including means to records made by any electronic form, magnetic form, or any other forms not recognizable to human perception) from the said Person, Executives and Personnel shall clearly indicate the purpose of use to the Person in advance, except for the following cases:
   (1) cases in which the acquisition of Personal Information is urgently required for the protection of life, body, or property of persons.
   (2) cases in which clear indication of the purpose of use to the said Person may damage the life, body, property, or other rights or interest of the said Person or a third party.
   (3) cases in which clear indication of the purpose of use to the said Person is likely to cause impediments to the proper execution of JAXA, other national organ, Incorporated Administrative Agencies, etc. or local public entities.
   (4) cases in which the purpose of use is obvious considering the circumstances of the acquisition.
2. Ways for indicating the purpose of use listed in the preceding Paragraph shall comply with the followings, depending on the means of acquisition.
   (1) Where the Executives and Personnel acquire the said Personal Information by Documents, etc. directly from a Person.
      a) Indication in an application form, etc. or Documents explaining how to fill in the form or a guidance, etc.
      b) Indication at a reception desk; provided, however, that this shall only apply
where a reception desk for accepting applications is set.

c) Indication by verbal explanation; provided, however, this shall only apply
where the above a) and b) are not possible or available.

(2) Indication in an application form, etc. or Documents explaining how to fill
in the form or a guidance, etc. where Executives and Personnel acquire said
Personal Information receiving by postal mail, etc.,

(3) Indication on an entry screen or Documents explaining how to fill in the
form or a guidance, etc. where Executives and Personnel acquire said
Personal Information by receiving a submission via magnetic means such as
online application system, etc.

Article 68 Restriction on Use and Securing the Accuracy

1. Executives and Personnel shall not Read, Copy, Remove, Lend, Provide and
Dispose (hereinafter referred to as "Use" in this Section) Retained Personal
Information for purposes other than intended purposes except for cases based on
Laws and Ordinances.

2. Executives and Personnel shall endeavor to maintain the Retained Personal
Information consistent with the past or present facts within the scope necessary
for the achievement of the purpose of Use.

3. When a mistake is found in the contents of Retained Personal Information,
Executives shall correct, etc. the Information in accordance with the instructions
of the Security Control Administrator.

4. Executives and Personnel shall, depending on the importance of the Retained
Personal Information handled by Information Systems, compare source
Information and entered contents, confirm contents of Retained Personal
Information before and after the processing, and compare with existing Retained
Personal Information.

Subsection 2 Management of Personal Information

Article 69 Management of "A" Personal Information

1. The provisions on management of "A" Information of Section 3 of this Chapter
shall apply mutatis mutandis to the management of "A" Personal Information.

2. Only the designated concerned persons may use "A" Personal Information
within the scope of the purpose of Use by taking procedures as stipulated in each
Article of Section 3 of this Chapter.

3. Notwithstanding the provision of the preceding Paragraph, when the Security
Control Administrator, etc. recognizes that some circumstance falls under any of
the followings, a concerned person may Use Retained Personal Information
other than the purpose of Use. However, this shall not apply where such Use
may improperly infringe the rights or interest of the Person or the third party.

(1) where a Person has agreed to the Use, or the Information is provided with
the said Person himself/herself.

(2) where using the Retained Personal Information within JAXA only to the
extent necessary for conducting duties under its jurisdiction provided by
Laws or Ordinances, and where there is a reasonable ground for such use.

(3) where the Retained Personal Information is provided with the administrative
organ (as prescribed in Article 2, Paragraph 1 of Act on the Protection of Personal Information Held by Administrative Organs: Act No. 58 of 2003. (hereinafter referred to as "Administrative Organ's Personal Information Protection Act"), other Incorporated Administrative Agencies, or local public entities in which the person who receives the Retained Personal Information uses it only to the extent necessary for executing clerical works or duties under its jurisdiction provided by Laws or Ordinances, and where there is a reasonable ground for such use of the Retained Personal Information.

(4) In addition to the cases listed in the preceding three Items, where the Retained Personal Information is provided exclusively for statistical purposes or academic research purposes, provision of the Retained Personal Information to other persons is obviously beneficial to the Person concerned, or there are other special grounds for providing the Retained Personal Information.

4. The provision of the preceding Paragraph shall not preclude the application of the provisions of other Laws or Ordinances restricting the use or Providing of Retained Personal Information.

5. The Security Control Administrator, etc. shall, when Lending or Providing the Retained Personal Information pursuant to preceding Paragraph 2, Paragraph 3 Item 3, or 4 to persons outside JAXA, impose on the said person the restriction on the purpose or method of use or any other necessary restrictions with regard to the Provided Personal Information, or request the said person to take necessary measures for the prevention of leakage and for the proper management of the Information.

Article 70 Exception to Handling of Emergency Contact Network, etc., etc. that Falls Under "A" Personal Information

1. Article 44 (Reading), 45 (Copying), and 46 (Removing) shall not apply to Emergency Contact Network, etc. provided for the use for contacts in emergency and telephone directory provided for use for contacts among persons concerned in the course of duties that fall under "A" Personal Information.

2. When Reading Emergency Contact Network, etc. outside the controlled area of the organization, Executives and Personnel shall pay attention to prevent it from peeping, and shall not allow persons except for concerned persons to Read Emergency Contact Network, etc.

3. When distributing Emergency Contact Network, etc. to users designated as concerned persons, one shall omit registration to a registry as a copy of the distributed Emergency Contact Network, etc. Executives and Personnel shall be careful not to let persons other than concerned persons have Emergency Contact Network, etc. by prohibiting Copying and adopting an indication of serial numbers.

4. When concerned persons take out Emergency Contact Network outside of the controlled area of JAXA, the Security Chief Administrator’s permission and registration to a registry may be omitted. When Removing Emergency Contact Network, etc. concerned persons shall carry it with them, and shall always pay attention not to lose or be stolen.
Article 71 Management of "B" Personal Information
1. The provisions on Management of "B" Information of Section 4 of this Chapter shall apply mutatis mutandis to the management of "B" Personal Information.
2. Only the designated concerned persons may use "B" Personal Information within the scope of the purpose of Use by taking procedures as stipulated in each Article of Section 4 of this Chapter.
3. Article 69, Paragraphs 3 to 5, Management of "A" Personal Information shall apply mutatis mutandis to the management of "B" Personal Information.

Article 72 Procedure for Disclosure of Personal Information
Provisions concerning disclosure of the Retained Personal Information and the report to the governing ministries shall be in accordance with "Regulation on the Disclosure of Personal Information" (Regulation #17-8.)
Chapter 4 Information Systems Security

Section 1 Information Systems Security Management
Article 73 Information Systems Security Measures
1. While assuring the convenience of Information Systems, security of Information Systems shall be ensured based on the importance of Information as stipulated in Chapter 3, which is contained in Information Systems, and the importance and results of risk assessment of duties for which Information Systems are used as stipulated in Chapter 6, in accordance with the following physical and technical countermeasures.
   (1) Physical countermeasures: Prevention against theft and loss of Information Systems such as computers, management of entry/exit of server rooms, etc.
   (2) Technical countermeasures: Access control using password, etc. recording access log, measures against computer virus and denial-of-service attacks, etc.
2. For the determination of criteria of each countermeasure listed in the preceding Items shall be followed as specified separately by the Information Systems Security Chief Administrator.

Article 74 Understanding of Information Systems Development and Operations Status etc.
Information Systems Division Administrator shall periodically compile the development and operation of Information Systems and report them to the Information Systems Security Chief Administrator.

Article 75 Measures for Information Systems Security Assurance
1. The Security Control Administrator of each Directorate and Department, etc. or the Information Systems Division Administrator shall limit or terminate operation of Information Systems, or take other necessary measures if he/she believes it specially necessary to assure the security of Information Systems.
2. The Security Control Administrator of each Directorate and Department, etc. or the Information Systems Division Administrator shall, when taken measures stated in the preceding Paragraph, report the facts to the Information Systems Security Chief Administrator.
3. The Information Systems Security Chief Administrator shall, when received the report stated in the preceding Paragraph, take necessary measures for each Information System.

Section 2 Information Systems Utilization
Article 76 Obligations of Information System Users
1. Executives and Personnel shall comply with the Act on the Prohibition of Unauthorized Computer Access (Act No.128 of August 13, 1999), other Laws or Ordinances, this provision and the provision of other organizations.
2. Executives and Personnel shall use Information Systems for the purpose of operating their duties.
3. Executives and Personnel shall take measures regarding Information Systems
security such as properly managing passwords.

4. Executive and Personnel shall receive the permission through the process set by Information Systems Division Administrator when they connect to the network, use Wireless LAN, bring in and out computers for the purpose of using Information Systems.

5. Executives and Personnel shall receive the permission through the process set by Information Systems Division Administrator when they connect to the network, conduct route change, set Wireless LAN router, move, bring in, bring out Information Systems and change the major system’s setting for the purpose of maintenance and operation of Information Systems.


Article 77 Prohibited Acts

1. Executive and Personnel shall not conduct the acts stipulated in the following Paragraphs at the time of maintenance, operation and use of the Information Systems.

   (1) Illegal access as stipulated in Act on the Prohibition of Unauthorized Computer Access (Act No.128 of August 13, 1999) and other illegal acts.

   (2) Acts, which impairs Information Systems security by changing the structure of Information Systems, which affect the security, use of inappropriate software and passwords in the course of duties, acts which prevent a regular operation of Information Systems.

   (3) Informing others of secrets and Personal Information which are obtained in the course of duties by using the Information Systems.

   (4) Damaging the reputation of JAXA or harming its interests or conducting acts, which disgrace Personnel as a whole by using Information Systems.

   (5) Violation of public order and moral such as accessing inappropriate websites.

   (6) Use Information Systems for personal purpose such as stock transactions and mail order purchasing.

   (7) Executives and Personnel shall not use Information Systems designated for separately by the Information Systems Security Chief Administrator (hereinafter called "Information Systems Outside of Work") such as personal Information Systems of Executives and Personnel, computers which are in public and used by a large number of people for conducting their duties. Information obtained in the course of duties, which excludes publicly known Information, shall not be loaded in Information Systems Outside of Work. Information Systems stated in this Section means computers, servers, workstations, USB flash drives and other external memory devices regardless of Item 7, Paragraph 1 of Article 3.

2. Personnel who are in charge of maintenance and operation of Information Systems shall not conduct acts stipulated in each Section of the preceding Paragraph and shall not Read Personal Information for without a good reason and inform others of Personal Information obtained through in the course of duties or use it for unjustified purposes.
Article 78 Investigation of Prohibited Acts

1. Personnel, who are in charge of maintenance and operation of Information Systems, shall regularly inspect Information Systems and report to Information Systems Security Chief Administrator in cases where there is a doubt that one of the Personnel conducts any of the prohibited acts stipulated in the preceding Article. The Information Systems Security Chief Administrator notifies the Security Control Administrator, etc. of Directorate and Department, etc. in which the said person belongs based on the said report.

2. The Security Control Administrator, etc. instructs Information Systems Division Administrator to investigate the current situation in cases where there is a doubt that a Personnel conducts prohibited acts stipulated in the preceding Article.

3. As a result of the investigation said in the preceding Paragraph, in the event that there is a reasonable grounds to believe that said Personnel conducts the prohibited acts stipulated in the preceding Paragraph, the said Personnel shall agree to be interviewed by the Security Control Administrator, etc.
Chapter 5 Security of Assets

Section 1 General Provisions of Security of Assets

Article 79 General Principles of Security of Assets

1. In order to ensure the security of tangible assets that belong to JAXA, the areas for which security should be ensured shall be controlled based on each category as stated in each Item of Article 80, Paragraph 1, according to its degree of critical risk assessment.

2. Category of each security asset shall be designated by the Security Control Administrator of each Directorate and Department, etc. or the Security Control Assistant Administrator who has been delegated its authority (note that for "AA" asset management, the Security Control Administrator’s delegation to the Security Control Assistant Administrator shall be limited to the Directors of each Department or above ranks as stipulated in Article 3 of the Decision-making Authority Regulation.) Every security asset shall be controlled as necessary according to its designated category.

3. Management of each security asset shall be conducted in accordance with the provisions in this Chapter and other regulations regarding asset management.

Article 80 Categorization of Tangible Assets

Among the tangible assets owned by JAXA, the security of which must be ensured, shall be controlled based on each category according to the degree of importance and results of risk assessment.

(1) "AA" assets

Among tangible assets to which only concerned Executives, Personnel and concerned external persons who have been deemed particularly necessary due to specific operational requirements may have access, and falls under any one of the following Items are designated as "AA" assets:

a) goods that include technology categorized as "AA" Information.

b) goods that have been imported based on international agreements and need strict control.

c) goods that if lost or damaged, would have a fatal effect on achieving the mission, or would tremendously damage the social credibility of JAXA.

(2) "A" assets

Among tangible assets to which only concerned Executives, Personnel, and concerned external persons who have been deemed necessary due to specific operational requirements may have access, and falls under any one of the following Items are designated as "A" assets:

a) goods that include technology categorized as "A" Information.

b) goods that have been imported based on international agreements and need certain level of control.

c) goods that if lost or damaged, would have a substantial effect on achieving the mission, or would damage the social credibility of JAXA.

Section 2 "AA" Assets

Article 81 Registration to "AA" Assets

1. An asset which has been designated as an "AA" asset shall have a defined scope
of concerned persons who may access said asset, and shall be registered in a registry. The scope of the concerned persons who may access "AA" assets that contain "AA" Information shall be the same with the scope of the concerned persons who have the authorization to access "AA" Information.

2. When designating an object as an "AA" asset, the scope of the designation shall be clarified and minimum.

3. The Security Control Administrator of each Directorate and Department, etc. or the Security Control Assistant Administrator who has been delegated its authority shall organize "AA" asset registry and conduct an internal audit regarding its management status once a year. The internal audit can be substituted by conducting its inventory count in accordance with the Guidelines on Asset Management.

Article 82 Storage and Service Space of "AA" Assets

1. Any security assets designed as "AA" assets shall be stored in Type I Controlled Area. Goods that are easily carried around shall be stored in a container with a key in Type I Controlled Area.

2. In principle, "AA" assets shall be used in Type I Controlled Area.

3. The Executives and Personnel shall, when have concerned external persons use "AA" assets, take measures equivalent to those stated in the preceding two Paragraphs.

4. The Executives and Personnel shall apply mutatis mutandis to the preceding two Paragraphs to ensure the security of assets that are likely to be designated as "AA" assets.

Article 83 Removal and Transportation of "AA" Assets

1. When it becomes inevitable to take an "AA" asset out of Type I Controlled Area for the purpose of implementing duties, the Executives and personnel shall take necessary protective measures including surveillance by the security guards. For goods that contain "AA" Information, measures shall be taken to guard the said "AA" Information from others.

2. When outsourcing transportation of "AA" assets from the controlled area, the Executives and personnel shall organize an emergency contact plan beforehand, store "AA" assets in a container, etc. with the key locked or sealed. In principle, the Removal and Transportation shall be conducted accompanied by the concerned persons.

Article 84 Disposal of "AA" Assets

When disposing an "AA" asset that is highly-confidential, the concerned persons of said asset shall take necessary measures to prevent the leakage of sensitive Information included in said asset.

Section 3 "A" Assets

Article 85 Registration to "A" Assets

When an asset is designated as an "A" asset, the scope of concerned persons who may access said asset shall be defined. The scope of the concerned persons who
may access "A" assets that contain "A" Information shall be the same with the scope of the concerned persons who have the authorization to access "A" Information.

Article 86 Storage and Service Space of "A" Asset
1. Any security assets designated as "AA" assets shall be stored in Type II Controlled Area. Goods that are easily carried around shall be stored in a container with a key in Type II Controlled Area.
2. In principle, "A" assets shall be used in Type II Controlled Area.
3. The Executives and Personnel shall, when Lending or having concerned external persons use "A" assets, apply mutatis mutandis to the preceding two Paragraphs.
4. The Executives and Personnel shall apply mutatis mutandis to the preceding two Paragraphs to ensure the security of assets that are likely to be designated as "A" assets.

Article 87 Removing and Transportation of "A" Assets
1. When it becomes inevitable to take an "A" asset out of Type II Controlled Area for the purpose of implementing duties, the Executives and personnel shall take necessary protective measures. For goods that contain "A" Information, measures shall be taken to guard the said "A" Information from others.
2. When outsourcing transportation of "A" assets from the controlled area, the Executives and personnel shall enclose "A" assets in a container, etc. with the key locked or sealed.

Article 88 Disposal of "A" Assets
When disposing an "A" asset, Article 84 shall apply mutatis mutandis.
Chapter 6 Security of Duties

Article 89 Duties Requiring Security Assurance

Of all duties conducted by JAXA, what particularly require security shall be implemented within the controlled areas in accordance with the followings which the Security Control Administrator of each Directorate and Department, etc. or his/her entrusted Security Control Assistant Administrator categorizes, based on the importance and results of risk assessment of such duties.

1) "AA" duties

Among rocket launch duties, tracking and control duties of artificial satellites, operation duties of aircrafts and testing duties related to the development of rockets, artificial satellites and aircrafts, what potentially has a fatal impact on JAXA in achieving its missions due to interference, etc. shall be categorized as "AA" duties and shall be implemented within Type I Controlled Area.

2) "A" duties

Among other duties than "AA" duties, what handles Information above "A" Information and what potentially has impact on JAXA in achieving its missions due to interference, etc. shall be categorized as "A" duties and shall be implemented within Type II Controlled Area.

Article 90 Duties Outside Controlled Areas

When duties requiring ensured security specified in the preceding Article become necessary to be conducted outside the designated controlled areas, necessary measures shall be taken in order to maximally secure security equivalent to the one in the designated controlled area in accordance with the classification.
Section 91 Categories and Designation of Controlled Areas

1. In order to ensure the security of corporate buildings and grounds that belong to JAXA (including annexed facilities, these are hereinafter collectively referred to as "Premises"), the areas for which security should be ensured (hereinafter referred to as the "Controlled Areas") shall be categorized as follows:

   (1) Type I Controlled Area
   Areas requiring particularly strict control to where only concerned Executives, Personnel and concerned external persons who have been authorized by the Security Control Administrator of each Directorate and Department, etc. or his/her entrusted Security Control Assistant Administrator, or Area Control Managers at offices etc. in which Area Control Managers are placed (hereinafter referred to as the "Area Control Manager, etc.") as deemed necessary for duties, may have access.

   (2) Type II Controlled Area
   Areas requiring strict control to where only concerned Executives, Personnel and concerned external persons who have been authorized by the Area Control Administrator, etc., as deemed necessary for duties, may have access.

   (3) Type III Controlled Area
   Areas to where only Executives, Personnel, and persons who have received Entry Permits at the reception desk may have access.

2. The security of Information, Information Systems, tangible assets, and duties shall be ensured as stipulated in the preceding Paragraph 1 and as shown in the table below.

<table>
<thead>
<tr>
<th>Controlled Area</th>
<th>Classification</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type I Controlled Area</td>
<td>Information</td>
<td>Storage/use of &quot;AA&quot; Information</td>
</tr>
<tr>
<td></td>
<td>Information Systems</td>
<td>Storage/use of Information Systems loaded with Information categorized as &quot;AA&quot; Information</td>
</tr>
<tr>
<td></td>
<td>Assets</td>
<td>Storage/use of &quot;AA&quot; assets</td>
</tr>
<tr>
<td></td>
<td>Duties</td>
<td>Implementation of &quot;AA&quot; duties</td>
</tr>
<tr>
<td>Type II Controlled Area</td>
<td>Information</td>
<td>Storage/use of &quot;A&quot; Information</td>
</tr>
<tr>
<td></td>
<td>Information Systems</td>
<td>Storage/use of Information Systems loaded with &quot;A&quot; Information</td>
</tr>
<tr>
<td></td>
<td>Assets</td>
<td>&quot;Storage/use of &quot;A&quot; assets</td>
</tr>
<tr>
<td></td>
<td>Duties</td>
<td>Implementation of &quot;A&quot; duties</td>
</tr>
</tbody>
</table>

3. The Controlled Areas stipulated in the preceding Paragraph 1 shall be designated by the Area Control Manager, etc. The Areas shall, in principle, be established in such a way that Type III Controlled Area shall be designated as the outermost boundary, with each Controlled Area surrounded by the Controlled Area of its
most immediate lower security level.

Article 92 Responsibilities of the Area Control Manager, etc.
1. The Area Control Manager, etc. shall, in accordance with the categories of the Controlled Areas, and as stipulated in each Section of this Chapter, shall take necessary measures, such as maintenance of protective walls, surveillance equipment etc., area entry management, such as keys, ID cards, etc., monitoring by security guards, and access control, etc.
2. The Area Control Manager, etc. shall take measures or give required instructions, such as prohibition of entry, if deemed necessary in order to ensure security in any Controlled Area.
3. The Area Control Manager, etc. shall not allow any acts that potentially threaten security within the Controlled Areas, such as entry into the Controlled Areas without permission (including acts of destructing equipment and devices installed for ensuring security.)
4. When any of the acts in the preceding Paragraph has happened, the Area Control Manager, etc. shall immediately take necessary measures, such as expulsion order to a person who engages in such act or suspension order or removal order of an item used for such act.
5. The Area Control Manager, etc. shall prescribe in the Implementation Guideline, etc. the methods of designation, protection, access control and other items necessary for the Controlled Area over which he/she has jurisdiction.

Article 93 Obligations of Executives and Personnel, etc.
1. Executives and Personnel, etc. shall always carry their IDs and Entry Permits, when entering any Controlled Area above Type III Controlled Area. They shall show their IDs and Entry Permits, when asked by the Area Control Manager, etc.
2. Executives and Personnel, etc. shall not enter without authorization, following someone that has unlocked the entrance, or shall not enter any Area by using an ID or Entry Permit of someone else. In addition, they shall not ask for entry permission or borrow any key under someone else's name.

Article 94 Area Entry in Emergency
When an emergency has happened, the Area Control Manager, etc. may allow the entry of fire vehicles, police vehicles, emergency vehicles for electricity/gas business and other vehicles and persons with special legal authority, into any Controlled Area, notwithstanding they don’t possess any Entry IDs or Entry Permits. In this case, the Area Control Manager, etc. shall, in principle, have any predetermined person that possesses an Entry ID attend the entry.

Article 95 Facilities Open to the Public
1. Opening the facilities to the public, including any events open to the public, shall in principle take place in a facility which does not fall under Type I to Type III Controlled Areas (hereinafter referred to as the "General Controlled Areas") or Type III Controlled Area.
2. Type II Controlled Area can be exceptionally opened to the public with the attendance of staff, after taking measures necessary for preventing leakage of
Information, destruction of assets and interference with duties under the permission of the Area Control Manager, etc.

3. When opening the facilities to the public, the Area Control Manager, etc. shall prepare a prevention/protection plan in advance and inform persons in charge of the opening and related Area Control Operations Managers. In addition, areas opened to the public shall be clearly shown to visitors, using guide maps, notice boards, ropes, etc.

4. For the purposes of conducting public relations and promoting understanding toward the activities of JAXA, if the requirements defined below are satisfied, unauthorized persons are exclusively allowed to enter Type I Controlled Area for other purposes than duties.

   (1) The said entry is deemed especially beneficial for Information providing and public relations activities to the citizens or promoting understanding toward the activities of JAXA.

   (2) If the said Area contains security objects that are highly-confidential assets of "AA" Information or "AA" assets, necessary measures shall be taken to prevent the occurrence of stealing, leakages etc. of Information and if such objects are assets with extremely high integrity and availability, necessary measures shall be taken to prevent from stealing, destruction etc.

   (3) Entry permission of the Area shall be obtained in advance in accordance with procedures defined for separately by the Area Control Manager, etc.

Section 2 Type I Controlled Area

Article 96 Protection of Type I Controlled Area

1. Type I Controlled Area shall be in principle established inside Type II Controlled Area, with its surroundings installed with sturdy enclosures, locked at all times. If the Area has openings, such as windows, such openings shall be reinforced to prevent easy penetration.

2. In Type I Controlled Area, a recording device, such as a surveillance camera, shall be installed in order to deal with Security Cases to protect Information and assets stored inside of said Area.

3. If multiple objects of security listed in Table in Paragraph 2 of Article 91 are stored within Type I Controlled Area, access control shall be thorough, by separately putting them into archives, storages, etc.

Article 97 Entry to Type I Controlled Area

1. The Area Control Manager, etc. shall designate concerned persons in advance those who are involved in the objects of security listed in Table in Paragraph 2 of Article 91 which are stored or implemented in Type I Controlled Area.

2. In principle, only designated concerned persons may enter Type I Controlled Area for the purpose of duties to be implemented in the said Area.

3. In Type I Controlled Area, records of entry/exit shall be left whenever an entry of or exit from the Area is made. The Area entry/exit shall be in principle controlled by electronic identification system.

4. When entering Type I Controlled Area, devices with an imaging function shall not be brought in without permission of the Area Control Manager, etc.

5. The Area Control Manager, etc., when he/she has been requested to permit entry
of Type I Controlled Area by unconcerned persons for the purpose of duties to be conducted in the said Area, may permit such entry after examining the purpose and contents of the work, the extent, condition, necessity, appropriateness etc. of the entry.

Article 98 Exceptions to Protection of Type I Controlled Area
When the Area Control Manager, etc. recognizes difficulty or inappropriateness in taking necessary protective measures in Paragraph 1 of the preceding Article for large structures, such as antennas installed outdoors which are classified as "AA" asset, he/she may designate such an area as Type I Controlled Area by enhancing necessary measures to protect the surrounding Type II Controlled Area.

Section 3 Type II Controlled Area
Article 99 Protection of Type II Controlled Area
Type II Controlled Area shall be in principle established inside Type III Controlled Area with its surroundings installed with sturdy enclosures, locked at all times. If the Area has openings, such as windows, such openings shall be reinforced to prevent easy penetration.

Article 100 Entry to Type II Controlled Area
1. The Area Control Manager, etc. shall designate relevant Executives and Personnel and concerned external persons in duties conducted in Type II Controlled Area.
2. In principle, only designated concerned persons and those who have been permitted by the Area Control Manager, etc. may enter Type II Controlled Area for the purpose of duties to be implemented in the said Area.
3. Entry to Type II Controlled Area shall be in principle controlled by electronic identification system.
4. Video or photo shooting in Type II Controlled Area requires permission of the Area Control Manager, etc.
5. The Area Control Manager, etc., when he/she has been requested a permit entry for Type II Controlled Area by unconcerned persons for the purpose of duties to be conducted in the said Controlled Area, may permit such entry after examining the purpose of necessity, appropriateness, etc. of the entry.

Section 4 Type III Controlled Area
Article 101 Protection of Type III Controlled Area
1. The condition of Type III Controlled Area shall be in such a way that unauthorized Personnel can not enter by the installed enclosures, such as fences in order to identify the boundary with General Controlled Areas or JAXA's uncontrolled areas.
2. Type III Controlled Area shall be in principle installed with devices detecting intrusions from outside and monitored at all times using surveillance cameras.
3. The Area Control Manager, etc. shall implement 24-hour security operations and develop a communication system so that intruders can be detected.
4. When an intrusion has been detected through the security operations in the Paragraph 2, the Area Control Manager, etc. shall immediately check the current status. If he/she has identified the intruder, he/she shall make a necessary notification in accordance with the predetermined Emergency Contact Network, etc.

Article 102 Entry to Type III Controlled Area
1. In principle, only Executives and Personnel and those who have been permitted by the Area Control Manager, etc. may enter Type III Controlled Area.
2. The Area Control Manager, etc., when he/she has been requested an entry permission to Type III Controlled Area, may permit the entry after confirming its purpose.

Article 103 Exceptions to Protection of Type III Controlled Area
1. When it is difficult for Type III Controlled Area to satisfy the protection requirements due to physical constraints, such as the shape of the land in the Premises for which Type III Controlled Area is to be established, or other constraints, such as laws and lease agreements, protective measures shall be taken to the extent possible and protective methods in Type II or above Controlled Area located inside the said Area shall be enhanced.
2. If the constraints in the preceding Paragraph make it difficult to maintain continuous monitoring by intrusion detection devices and surveillance camera images or conduct security operations in emergency response when an intrusion has been detected, alarms or images recorded for a certain period of time may be the alternative.
Chapter 8 Security Education

Article 104 Security Education and Training

1. The Security Chief Administrator shall provide education and training regarding security control to Executives and Personnel periodically or temporarily. Note that education and training regarding Information security management shall be provided by the Information Systems Security Chief Administrator.

2. The Security Chief Administrator, etc. shall formulate and conduct the security education and training plan to Executives and Personnel every fiscal year.

3. Executives and Personnel shall participate in the security education and training as stipulated in the preceding Paragraph 2.

4. The Security Chief Administrator, etc. shall report the implementation status and the outcome of the security education and training to the Board.
Chapter 9 Security Auditing

Article 105 Security Auditing

1. The Security Chief Administrator shall conduct audits regularly or as necessary regarding security management. Auditing regarding Information security management shall be conducted by the Information Security Chief Administrator.
2. The Security Chief Administrator etc. shall create security auditing plan every fiscal year and conduct audits in accordance with the plan.
3. The Executives and Personnel shall cooperate with the auditing.

Article 106 Inspection of Personal Information

The Security Control Administrator shall prepare the Personal Information Protection Inspection Plan every fiscal year for his/her responsible recording media, processing route, storage of Retained Personal Information, conduct the inspection according to the plan, and if deemed necessary, report the results to the Security Chief Administrator.

Article 107 Reporting Auditing Results

1. The Security Chief Administrator or the Information Systems Security Chief Administrator shall report the results of the security auditing and Personal Information inspection to the Board.
2. The Security Chief Administrator or the Information Systems Security Chief Administrator shall, when he/she finds it necessary based on the results of audit and Personal Information inspection, implement measures for ensuring security.
Chapter 10 Security Measures Under Contract

Article 108 Security Measures Under Contract Duties
1. When JAXA enters into a contract, the Executives and Personnel shall obligate the contractor (including subcontractors; the same shall apply hereinafter) to comply with this regulation and JAXA’s other security rules to ensure its security as listed in the following Paragraphs and also specify a provision in the event of any breach of the security obligation.
   (1) Executives and Personnel shall, when having a contractor use Information categorized as "A" Information or higher levels, obligate the contractor to take same level of measures with JAXA’s regulations; which includes confidentiality, requiring JAXA’s permission for Copying, disclosing to, and Providing with third persons and paying special care for the storage.
   (2) Executives and Personnel shall, when having a contractor use Information categorized as "B" Information or higher levels, require JAXA’s permission for Copying, disclosing, and Providing to third persons and pay special care for the storage.
   (3) With regard to Information Systems handling Information listed in the preceding two Items, same level of security measures such as antivirus and prohibition of file-sharing software use, etc. Same shall be applied for an asset containing the Information categorized as "B" Information or higher levels.
   (4) Executives and Personnel shall, when having a contractor enter into the Controlled Area of JAXA for performing his/her duties, ask for the permission and have them follow JAXA’s Area Control Manager’s instructions.
2. JAXA shall, when entering into a contract such as an appointment and other forms of contracts with an individual to whom the Working Regulation and the Special Working Regulation are not applicable, apply mutatis mutandis to the Items of the preceding Paragraph.
3. JAXA shall, when accepting undergraduate students, graduate students, and interns, apply mutatis mutandis to the preceding Paragraph 1, and take necessary measures to ensure the security including access limitation to its tangible asset, Information, and Information Systems and implementation of security education.

Article 109 Outsourcing of Duties that Includes Personal Information Handling
1. In addition to the preceding Article, the Executives and Personnel shall, when outsourcing duties handling JAXA’s Retained Personal Information (including the case of acquisition of Personal Information in the name of JAXA; the same shall apply hereinafter,) select a person who is able to properly manage the Personal Information.
2. The Executives and Personnel shall, when having the consigner conducts the duties listed in the preceding Paragraph 1, specify the Items below and each Item of Paragraph 1 of the preceding Article in the contract. In addition, the Executives and Personnel shall confirm the consigner of necessary matters including its management system and inspection system on the control status of Personal Information.
(1) Duty of confidentiality regarding Personal Information  
(2) Limitation or condition on re-consignment  
(3) Limitation on Copying Personal Information  
(4) Response to the occurrence of Personal Information leakage  
(5) Deletion and return of Personal Information and its recording media  
(6) Cancellation of contract, compensation for damage, and other necessary matters in the case of a breach of contract  

3. Executives and Personnel shall, when having dispatched workers conduct duties handling Retained Personal Information, specify the duty of confidentiality, including Personal Information handling on worker dispatch contract.
Chapter 11 Responses to Security Cases

Article 110 Responses to Security Cases, etc.
1. The Security Control Administrator of each Directorate and Department, etc. shall establish the emergency response organization in preparation for the occurrence of any Security Cases.
2. When Executives and Personnel find any case that is relevant to the Security Case, he/she shall immediately take tentative measures and give a first report to the Security Control Administrator of Directorate and Department, etc.
3. The Security Control Administrator of each Directorate and Department, etc., if necessary, shall undertake appropriate measures including implementation of the emergency response organization. Unless obviously unrelated to Security Cases, the Security Control Administrator shall report the fact to the Security Chief Administrator, etc. and receive necessary instructions.
4. When a Security Case occurs, the Security Control Administrator of each Directorate and Department, etc. shall investigate the fact, determine the cause of the case, take preventive measure, compile them and report the case to the Security Chief Administrator, etc.
5. The Security Chief Administrator, etc., if necessary, shall instruct the Security Control Administrator of each Directorate and Department, etc. to investigate the case and take necessary measures to prevent similar cases. For the critical Security Case, the Security Chief Administrator, etc. shall report the case to the President of JAXA.

Article 111 Countermeasures for Cases Including Personal Information Leakage
1. The Security Control Administrator of each Directorate and Department, etc. shall, in cases where any critical Security Cases occur including the Personal Information leakage, investigate and announce the fact, deliberate necessary countermeasures to prevent the recurrence and announce the prevention plan.
2. The President of JAXA shall, when receives a critical Security Case including the Personal Information leakage, investigate and announce the fact, deliberate necessary countermeasures to prevent the recurrence and announce the prevention plan.

Article 112 Disciplinary Actions, etc.
1. When a Security Incident occurs as stipulated in Article 3, Paragraph 1, (11), disciplinary actions shall be taken based on the Working Regulation and Special Working Regulation, according to the severity of the contravention.
2. The Security Chief Administrator, when receives a report regarding a security case and determines to fall under "Security Incident", shall report to the Director of Human Resources Department in order to take a measure as stipulated in the preceding Paragraph 1.
Chapter 12 Miscellaneous Provisions

Article 113 Delegated Tasks
The Security Chief Administrator, the Information Systems Security Chief Administrator, or the Security Control Administrator may, with the approval of the President of JAXA, delegate the tasks stipulated in this regulation to other appropriate Executives and Personnel by instructing the necessary matters.

Article 114 Exceptional Measures
1. The Security Chief Administrator may, when deemed particularly necessary for ensuring the security of JAXA, restrict access to security areas or objects and take any other necessary measures.
2. The Security Control Administrator finds an urgent necessity to access security areas or objects and recognizes that there is a risk of impairing smooth and proper execution of duties if taking procedures stipulated in this regulation, he/she may, on a temporary basis, permit at his/her discretion the third party to access the subject security matters within the extent that do not interfere the assurance of the security notwithstanding this regulation.
3. When an exceptional measure as stipulated in the preceding Paragraph 2 has been taken, recording in a ledger and other necessary procedures are required subsequently.

Article 115 Access to Security Areas for Auditing
The Security Chief Administrator, the subordinates, and those to whom the authority has been delegated may access Information, Information Systems, tangible assets, and duties, and may enter into each Controlled Area which are all subjected to be secured as stipulated in Article 5, without the permission from the Security Control Administrator, etc. of each Directorate and Department, etc. or the Area Control Manager, etc., if their purpose is based on Article 105 "Security Auditing", Article 78 "Investigation of Prohibited Acts", Article 110 "Responses to Security Cases, etc." and is to take measures as stipulated in the preceding Article, Paragraph 1. Even in these cases, they may not touch confidential contents of the Information, tangible assets, and the duties.

Article 116 Others
Any necessary matters concerning the execution of this regulation shall be provided for separately by the Director of the Security Administration Office or the Director of the Information Systems Department through adjustments at the Board.
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.

Supplementary Provision (April 14, 2009: Regulation #22-32)
This set of regulations shall be enacted on April 14, 2009.

Supplementary Provision (November 30, 2011: Regulation #23-53)
This regulation shall come into effect as from April 1, 2012.

1. For the enforcement of this Regulation, terms written in the Regulations besides this Regulation, decisions of the President of JAXA and Executive Directors of each Directorate, Notices, and decisions of Directors of each Department shall be deemed to be replaced as follows.
"Information Security Regulations" or "Information Systems Security Regulation"
shall be read as "Security Regulation."
"Information Security Administrator" and "Executive Director and Director of each Directorate and Department, etc." regarding the security of tangible assets and duties shall be read as "the Security Control Administrator."
"Secret Information", "Information limited to authorized staff", and "Information limited to JAXA employees" shall respectively read "AA" Information, "A" Information, and "B" Information; the same shall apply to labels on the JAXA Documents.

2. "Information Security Regulation" (Regulation #15-48), "Information Systems Security Regulation" (Regulation #15-49), and "Regulation on the Control of Special Imported Equipments" (Regulation #15-52) are all hereby abolished.

3. For the enforcement of this Regulation, if changes are only of Regulation names, position names, and Information Category written in other Regulations, decisions of the President of JAXA and Executive Directors of each Directorate, and Notices and decisions of Directors of each Department as stipulated in Article 3 to Article 7 of the "General Regulation" (Regulation#15-1), the changes shall be deemed to be amended by the enforcement of this Regulation.

4. Documents which have been designated as the "Handling Attention Documents" in accordance with the Document Management Regulation (Regulation#15-21) in the past, shall be deemed to be designated as "B" Information as stipulated in Article 26, Paragraph 1 of this Regulation.
5. 凡例  
5.1 役職名等の用例

<table>
<thead>
<tr>
<th>日本語</th>
<th>本翻訳中の英文名称</th>
</tr>
</thead>
<tbody>
<tr>
<td>理事長</td>
<td>President</td>
</tr>
<tr>
<td>セキュリティ統括</td>
<td>Security Chief Administrator</td>
</tr>
<tr>
<td>情報システムセキュリティ統括</td>
<td>Information Systems Security Chief Administrator</td>
</tr>
<tr>
<td>セキュリティ会議</td>
<td>Security Board</td>
</tr>
<tr>
<td>セキュリティ担当理事</td>
<td>Executive Director for Security</td>
</tr>
<tr>
<td>情報化担当理事</td>
<td>Executive Director for Information</td>
</tr>
<tr>
<td>情報化統括</td>
<td>Senior Chief Officer of Information</td>
</tr>
<tr>
<td>情報システムセキュリティ部会</td>
<td>Information Systems Security Committee</td>
</tr>
<tr>
<td>セキュリティ統括補佐</td>
<td>Security Assistant Chief Administrator</td>
</tr>
<tr>
<td>情報システムセキュリティ統括補佐</td>
<td>Deputy Information Systems Security Chief Administrator</td>
</tr>
<tr>
<td>情報システムセキュリティ統括補佐</td>
<td>Information Systems Security Assistant Administrator</td>
</tr>
<tr>
<td>セキュリティ統括管理責任者</td>
<td>Security Control Administrator</td>
</tr>
<tr>
<td>セキュリティ統括管理責任者補佐</td>
<td>Security Control Assistant Administrator</td>
</tr>
<tr>
<td>セキュリティ担当者</td>
<td>Security Control Staff</td>
</tr>
<tr>
<td>エリア管理責任者</td>
<td>Area Control Administrator</td>
</tr>
<tr>
<td>エリア管理実施責任者</td>
<td>Area Control Operations Managers</td>
</tr>
<tr>
<td>情報システム部署責任者</td>
<td>Information Systems Division Administrator</td>
</tr>
<tr>
<td>情報システム部署管理者</td>
<td>Information Systems Division Manager</td>
</tr>
<tr>
<td>情報システム責任者</td>
<td>Information Systems Administrator</td>
</tr>
<tr>
<td>情報システム管理者</td>
<td>Information Systems Manager</td>
</tr>
</tbody>
</table>

※上記用例は、規程内容の理解しやすさを優先し、役職名の階層等が容易にイメージできる単語を用いており、必ずしも機構内で通常使用されている用例に一致しない場合がある。
5.2.用語の用例

<table>
<thead>
<tr>
<th>日本語</th>
<th>本翻訳中の用語の英訳</th>
</tr>
</thead>
<tbody>
<tr>
<td>移管</td>
<td>Transferring</td>
</tr>
<tr>
<td>閲覧</td>
<td>Reading</td>
</tr>
<tr>
<td>開示</td>
<td>Disclosure</td>
</tr>
<tr>
<td>各部署</td>
<td>Divisions</td>
</tr>
<tr>
<td>各本部・部等</td>
<td>Directorates and Departments</td>
</tr>
<tr>
<td>貸出し</td>
<td>Lending</td>
</tr>
<tr>
<td>管理区域</td>
<td>Controlled Area</td>
</tr>
<tr>
<td>機構</td>
<td>JAXA</td>
</tr>
<tr>
<td>規程</td>
<td>regulation</td>
</tr>
<tr>
<td>業務</td>
<td>Duties</td>
</tr>
<tr>
<td>業務外情報システム</td>
<td>Information Systems Outside of Work</td>
</tr>
<tr>
<td>緊急の事態</td>
<td>emergency</td>
</tr>
<tr>
<td>緊急連絡網</td>
<td>Emergency Contact Network</td>
</tr>
<tr>
<td>個人情報</td>
<td>Personal Information</td>
</tr>
<tr>
<td>再委託</td>
<td>re-consignment</td>
</tr>
<tr>
<td>社屋等</td>
<td>Premises</td>
</tr>
<tr>
<td>情報</td>
<td>Information</td>
</tr>
<tr>
<td>情報システム</td>
<td>Information Systems</td>
</tr>
<tr>
<td>情報システムセキュリティ</td>
<td>Information Systems security</td>
</tr>
<tr>
<td>情報システムセキュリティ部会</td>
<td>Information Systems Security Committee</td>
</tr>
<tr>
<td>情報セキュリティ</td>
<td>Information Security</td>
</tr>
<tr>
<td>職員</td>
<td>Personnel</td>
</tr>
<tr>
<td>正確性の確保</td>
<td>Securing the Accuracy</td>
</tr>
<tr>
<td>セキュリティ会議</td>
<td>Security Board</td>
</tr>
<tr>
<td>セキュリティ監査</td>
<td>Security Auditing</td>
</tr>
<tr>
<td>セキュリティ事案</td>
<td>Security Case</td>
</tr>
<tr>
<td>セキュリティ事故</td>
<td>Security Incident</td>
</tr>
<tr>
<td>セキュリティ統括等</td>
<td>Security Chief Administrator/ Information Systems Security Chief Administrator.</td>
</tr>
<tr>
<td>セキュリティ統括管理責任者等</td>
<td>Security Control Administrator/ Security Control Assistant Administrator</td>
</tr>
<tr>
<td>提供</td>
<td>Providing</td>
</tr>
<tr>
<td>点検</td>
<td>Inspection</td>
</tr>
<tr>
<td>廃棄</td>
<td>Disposing</td>
</tr>
<tr>
<td>秘密情報等</td>
<td>secret Information etc</td>
</tr>
<tr>
<td>複製</td>
<td>Copying</td>
</tr>
<tr>
<td>保有個人情報</td>
<td>Retained Personal Information</td>
</tr>
<tr>
<td>本人</td>
<td>Person</td>
</tr>
<tr>
<td>明示</td>
<td>Indication</td>
</tr>
<tr>
<td>持出し</td>
<td>Removing</td>
</tr>
<tr>
<td>役職員</td>
<td>Executives and Personnel</td>
</tr>
<tr>
<td>有形資産</td>
<td>Tangible Assets</td>
</tr>
<tr>
<td>要保護情報</td>
<td>Information Requiring Protection</td>
</tr>
</tbody>
</table>