Authority: Approved by the President

# Chapter 17: Information Technology and Security

## 17.1 Policy

This policy is in place to ensure that OIST Information Technology Resources (IT resources) are provisioned and used in an effective, efficient, prudent and responsible manner, in line with the missions of the University and in compliance with relevant legal and contractual obligations. All users are expected to be familiar with these policies, rules and procedures and consequences of violation.

All University information is deemed to comprise University information assets. The University owns and controls its information assets. Appropriate handling of information assets is vital to the protection of OIST and its community, all users are responsible in this regard.

Though the University takes reasonable security measures to protect the security of its IT resources, the University does not guarantee absolute security nor privacy. The University has the right to monitor any and all IT Resources and their usage, including e-mail, without limitation. The University is responsible for taking any measures necessary to ensure the security and integrity of its IT Resources. When it becomes aware of violations of policy or law, either through routine system administration activities or via incident notification, it is the responsibility of the University to investigate as needed or directed, and take action to protect its resources and/or to provide information relevant to an investigation.

OIST has an obligation to preserve Information Assets for archival and reporting purposes. Additionally, upon direction from the President or General Counsel and upon consent of Chief Information Officer (CIO) and Chief Information Security Officer (CISO), Information Assets may sometimes be preserved for prescribed periods of time for litigation or other legal purposes.

IT Resources are not to be used for personal or private purposes unrelated to the mission of the University. However, incidental personal use is permitted so long as such use does not interfere or conflict with the employee's work responsibilities or other obligations to the University, and does not generate additional direct cost to the University. Users are responsible for the content of their personal communications. The University accepts no responsibility or liability for unauthorized use of its IT resources in a manner which does not comply with policy or law. All communications must comply with the OIST Email & Online Communication Code of Practice.

## 17.2 General Considerations

### 17.2.1 Scope

These policies, rules and procedures are applicable to all users. In particular, all users are subject to the requirements as set out under "User's Rights and Responsibilities" and the "OIST Graduate University IT Acceptable Use Policy".

In accessing, storing or transmitting University Information all IT Assets become subject to these policies. This includes personal devices, devices wholly or partially owned by the University, and devices from external organizations or entities.

### 17.2.2 Ownership of Information Assets

The University owns and controls its information assets. The University assigns responsibility for managing and protecting its Information Assets, and ensuring compliance with policy and law, to Information Asset Managers and Information Asset Administrators.

Within research units the Faculty serves as Information Asset Manager, and may assign the Information Asset Administrator role to a unit member. Ensuring appropriate management and security schemes for unpublished research data is the prerogative of the faculty, whom must also take into account any pre-existing official agreements that would require additional security or protection of information assets. Note that a primary copy of all research data should remain on OIST managed repositories at all times.

Within Divisions the Vice-President services as Information Asset Manager, and may assign the Information Asset Administrator role to one or more Section members.

Corporate Documents and Personal Information are a sub-set of Information Assets, but have additional legal and policy requirements, such as "Public Document Policy Act" and "Law concerning Access to Personal Information Held by Independent Administrative Institutions", associated with their handling. These requirements as well as separate management and administration roles are detailed here [Chapter 12].

Intellectual property, institutional agreements, or other contractual requirements upon the University may modify the ownership and treatment of information assets, these are covered under PRP Chapter 4 and Chapter 14.

### 17.2.3 Principles of Information Technology Management

Wherever possible University IT resources are to be provisioned in alignment with industry best practice. To this end the ITSM framework is employed to provide a structure in which to describe and specify IT services.

Core to the ITSM framework is the concept of a Service Level Agreement (SLA), which acts to provide clear expectations in the scope, timeliness and quality of IT services between IT Division and the University. This SLA must be drafted in conjunction with stake holders from all areas of the University. This SLA must be deliberated upon and approved by stake holders from all areas of the University as deemed necessary by the CIO, via the IT Strategy Committee.

### 17.2.4 Principles of Information Security

The purpose of information security is to protect Information Assets from unauthorized access or damage, and ensure accordance with all applicable laws, regulations and compliance requirements [Link: 17.8.8].

### 17.2.5 Further Policies Rules and Procedures

Research units, Divisions or Sections within the University may impose additional conditions of use upon IT Resources or facilities under their control. Such conditions must be consistent with this overall policy. They may provide additional detail, guidelines or greater restrictions. They may not provide lesser restrictions.

### 17.2.6 Communications and Public Relations

Other standards and rules developed by the Vice President for Communication and Public Relations apply to use of University IT with regard to e-mail, websites, and social media; compliance with those standards and rules is mandatory.

### 17.2.7 Students

Students should refer to the Graduate School Handbook in addition to familiarizing themselves with this chapter.

### 17.2.8 General Conduct

Beyond the policies and procedures regarding usage of the IT Resources as detailed herein, all users are expected to exercise sound judgment, and in situations where policy or procedure is unclear are expected to contact IT Division or the relevant party to seek clarification.

### 17.2.9 Compliance

Any breach of information security, or misuse of IT Resources is regarded as serious. Breaches may result in disciplinary action, up to and including dismissal and legal action.

## 17.3 Rules

### 17.3.1 Authorization and Access

All access to, and usage of IT resources must be appropriately requested, approved, registered and audited. A user is defined as any individual or entity granted access to OIST information assets to a level above public classification, or to IT resources above that available to the general public.

Users are responsible for protecting their account information by ensuring that their login, password and other access credentials remain secure at all times. The sharing of account information or passwords is not permitted, and may only be known to, and used by the individual assigned them.

In using these resources, users agree to abide by all relevant University policies, rules, procedures and applicable law. Users must acknowledge this understanding by reading and signing the OIST Graduate University Acceptable Use Policy, via physical signature or digital equivalent.

#### 17.3.1.1 Account Creation

User accounts will be created via the following process:

- Onboarding into the University via the process relevant to the user's classification, resulting in registration into the OIST Identity Management System
- Acknowledgement by signature (or digital equivalent) of the OIST Graduate University Acceptable Use Policy
- Supervisors' advance authorization to access any IT resources beyond those allocated by default
- Authorization by the relevant Information Asset Manager or Information Asset Administratorto access any Information Assets managed locally

#### 17.3.1.2 Account Extension

Requests for extension of access shall be made with valid justification, via the process relevant to the user's classification. Extension processes will include at least a minimum of supervisors' approval, and any further approvals as required.

#### 17.3.1.3 Account Expiry, Deactivation and Deletion

Accounts will be automatically deactivated upon expiry of a user's term at the University unless extended as described above.

Systems administrators must deactivate invalid accounts when found, or as instructed by the CIO, CISO or legal counsel, and report the event to CISO.

#### 17.3.1.4 Access Rights

Should users change roles or responsibilities, supervisors are responsible for ensuring updated access rights are communicated to IT Division, and any relevant Information Asset Managers. Information Asset Managers are responsible for ensuring that access rights are updated appropriately.

#### 17.3.1.5 Privileged Users/Systems Administrators

Any user granted escalated privileges must use them only when required to do so in order to conduct OIST business. System access events of users possessing escalated privileges are to be recorded and monitored at all times.

#### 17.3.1.6 Shared Accounts

Shared accounts are not in principle permitted, exceptions may be made at the discretion of the system administrators, with concurrence of the CIO or CISO.

#### 17.3.1.7 Unauthorized Access

All users, including system administrators, must report unauthorized access to the CISO immediately if suspected.

### 17.3.2 Bring Your Own Device (BYOD)

The University does not require personnel to use their personal resources to conduct University business.

Within the administration, the usage of personal IT assets to conduct OIST business is permitted only with the authorization of IT Division.
Within research units, the faculty may choose to permit the use of BYOD devices, and users may elect to use their own resources accordingly, though at no time should any user be compelled to do so. The University accepts no responsibility or liability for damage to BYOD devices. The faculty and asset owner are accountable for any and all issues arising from the usage of such personal assets.

Note that in connecting a personal IT asset to the OIST network (BYOD), or using a personal asset to store or transmit University Information, the asset is then subject to this policy and must comply with all OIST requirements. In the case of BYOD devices, eligibility to store OIST information assets may vary. Users are required to ensure that OIST information assets, the devices used to access them, and the mode of access conform to OIST information classification and device eligibility criteria.

### 17.3.3 Connecting to the OIST Network

The OIST network is an essential research resource, maintaining its availability and security is vital to the function of the University and is the responsibility of all users. All IT assets connecting to the OIST network must do so via OIST network authentication, uniquely identifying the active user. Users may only connect OIST IT assets for which they have authorization to use to the OIST network, and only for their own use. The connection of assets to the OIST network for the use of other users, or third parties is strictly prohibited.

Where network authentication poses a barrier to research or OIST business, users must contact IT Division to seek an exception. The connection of any devices that would bypass or mitigate network authentication, or enable other devices to do so, is strictly prohibited.

In order to ensure the security and stability of the OIST network, the connection of network devices, such as switches, routers or hubs without the authorization of IT Division is strictly prohibited. The usage of any wireless networks other than those provided by IT Division within OIST facilities without prior permission of IT Division is not permitted. Any unauthorized devices found to be connected to the OIST network, or providing wireless networking within OIST facilities may be disconnected without notice.

### 17.3.4 Procurement, Outsourcing and IT Assets

OIST IT Asset purchases must be fit for purpose. They must also be procured, audited, re-used and disposed of appropriately. In addition to University procurement policy, rules and procedures [Chapter 28], the purchase of IT Assets are also subject to the rules herein.

Regardless of procurement path or budget, all IT assets procured, donated to or otherwise received by OIST must be physically inspected by IT Division staff upon receipt. This inspection will include indelible asset marking (exceptions to which must be approved by CIO), and registration into the Configuration Management Database (CMDB) to allow for the efficient tracking and auditing of assets.

Exemptions may exist where the IT asset is an integral part of a larger research device or apparatus, i.e. a control PC bundled with a microscope. In this case the party receiving the asset is to coordinate with IT Division.

Consultation with IT Division is required before the purchase of any IT asset intended to be housed in IT Division facilities (server rooms, network spaces etc.) [Link: 17.3.30].

#### 17.3.4.1 Procurement of IT Assets within the Administration

Within the administration, including the Research Support Division, the procurement or upgrade of any IT asset (including any software procurement with a price above a 10,000yen) must be conducted via IT Division. This is to ensure standardization where applicable, and to ensure the devices are purchased in an efficient fashion. The procedure for requesting the purchase or upgrade of an IT device within the administration is detailed at PRP 17.5.1.

All IT assets within the administration fall under control of the IT Division, and are subject to this policy regardless of how they were acquired or funds used to purchase them.

#### 17.3.4.2 Procurement of IT Assets within Research Units

Research units are strongly encouraged to consult with IT Division before purchasing any IT asset. Where the research unit elects to purchase without consultation, the level of support IT Division can deliver to the IT asset may be limited. Connectivity with OIST networks is not guaranteed in this case. The support levels available to the various device categories are detailed in the SLA. The procurement process for IT assets within research units is covered under PRP 17.5.3.

IT assets to be procured as part of a larger research equipment purchase, or to be attached to research equipment should be specified with thought to reliability and performance. The reliability of these assets has substantial impact on the productivity of critical research equipment. Guidelines for specifying these purchases are part of the process for procurement of IT assets within research units [Link: 17.5.3].

#### 17.3.4.3 Procurement of IT Assets via Corporate Credit Card

The purchase of IT assets using corporate credit card (P-Card) is restricted, please see PRP 26.3.7. The purchase of IT assets from online vendors can only be conducted via IT Division.

#### 17.3.4.4 IT Asset Tracking

All IT assets which are wholly or partially owned by the university are to have the OIST asset tracking agent installed. This agent allows for the dynamic audit of IT assets, resulting in substantial savings in costs and personnel time during mandatory yearly asset audits. This requirement is mandatory for all assets in the administration, and strongly advised for assets within research units.

#### 17.3.4.5 IT Asset Transfer

The transfer of usage or ownership of any IT device, including between users, sections or research units, must be conducted via IT Division. In this way the asset register and CMDB is kept up to date, and data in the devices is securely erased prior to transfer to prevent breaches in security or personal information protection. The process for transferring an asset between users or sections and units is described at PRP 17.5.5.

#### 17.3.4.6 IT Assets Outside of OIST Premises

Where any IT asset is to be taken off-site, including for the purposes of business trips or working from home, prior authorization must be given by IT Division. In the case of laptops and mobile devices this authorization is normally incorporated into the agreement signed by the user upon physical issuance of the device [Link: 17.5.4].

#### 17.3.4.7 IT Asset Disposal

The disposal of all OIST IT assets must be conducted via IT Division, regardless of how they were acquired or the nature of the funds used to purchase them or if they are partially or wholly owned by OIST.

#### 17.3.4.8 IT Asset Theft, Loss or Damage

Users must report the loss, theft or damage of any IT Asset to the IT Helpdesk promptly [Link: 26.3.3].

### 17.3.5 Enterprise Applications

An enterprise application is defined as any administrative system key in conducting University business. The functionality and quality of these systems can have substantial impact on University business productivity. The design and implementation of such system must be performed with due diligence, in consultation with the IT Division, and via the mandatory process detailed at PRP 17.5.7.

### 17.3.6 Outsourcing of IT Services

Where contracting with an external party to provide a service or system that will store, transmit or receive OIST information assets, additional consideration must be given to the factors below. This is atop the procurement processes as detailed in PRP Chapter 28, and the enterprise application review process.

- A service level agreement (SLA) between OIST and the service provider.
- A non-disclosure agreement and other restrictions preventing the utilization of OIST Information assets for purposes other than those intended.
- The maturity of information security process within the service provider. Management structures within the service provider and its infrastructure which will protect OIST information assets from unintended changes by third parties, including subcontractors.
- OIST's right to audit the service provider's compliance with the contractual and security requirements.
- Regular monitoring and reporting to OIST on information security performance.

### 17.3.7 Outsourcing and Information Security

Where the operation or maintenance of a system or service is outsourced, the system owner shall be responsible for monitoring compliance with OIST information security requirements, reporting any discrepancies to the CISO.

In the case of information security incident or misuse of the system, the system owner or CISO may suspend the outsourced service. The procedure for the suspension of service, and correct allocation of authorizations to allow this shall be granted to the CISO by the system owner.

The system owner shall ensure that all information assets handed over to the outsourcer during the course of the contract are duly retrieved or destroyed at the appropriate point on or before termination of the contract.

Where the operation or maintenance of a system or service is outsourced, those matters stipulated in OIST Guidelines for Personal Information Protection [Chapter 11] must be adhered to.

### 17.3.8 Software and licensing

IT Division provides a wide range of research and business software to OIST users. Users are encouraged to use these software, but must respect copyright law and licensing restrictions at all times.

Software titles held by IT Division are in general only eligible for installation onto IT assets wholly owned by the University, users must not install software onto an IT asset without first confirming the IT asset is eligible. Details of available software and licensing restrictions are covered as part of the software catalog.

Within the administration the use of software outside the software catalog is not permitted. Where additional software is required, users must contact IT Division to request an addition to the catalog.

Within research units the use of software outside the software catalog is permitted, though consideration must be given to security. In using software outside the software catalog users should:

- Ensure the software has been downloaded from known reputable sources, such as the official website
- Ensure security patches are applied

#### 17.3.8.1 Licensed or commercial software

IT Division manages all commercial or licensed software within the administration, and many of the research software titles. Research units are strongly encouraged to contact IT Division before purchasing additional software. If there is general and continuing interest in a software product not yet offered in the software catalog, IT Division will research the request to see if we can negotiate an agreement that will best benefit the University.

#### 17.3.8.2 Open-source software and freeware

Within research units users are encouraged to use open source software and freeware, but are also encouraged to consult with IT Division. Where there is a continuing interest in a software title IT Division will package the software, manage updates and monitor security alerts and issues.

### 17.3.9 Information Asset classification

Information Asset manager shall assign information assets into one of the four classifications listed below, based upon determined value, confidentiality, integrity and availability. Where information assets with different levels of classification are grouped together, the highest classification shall be applied.
Further guidance on the handling of information assets is detailed under PRP 17.8.9 "information classification and device eligibility".

#### 17.3.9.1 Public

Information assets assigned the 'Public' classification should either be by their nature a matter of public record, or have been deemed safe to be publicly disclosed or to provide positive or neutral impact to OIST business, reputation or personnel.

#### 17.3.9.2 Internal

Information assets to be assigned the 'Internal' classification are those for which disclosure is not appropriate, and may result in a moderate negative impact to OIST business, reputation or personnel. These assets are to be made accessible to OIST users on a need to know basis. Unpublished research data or papers are in general deemed to fall under this classification.

Third parties may be granted access to information assets with an 'Internal' classification where a business need exists.

This classification should be regarded as the default for OIST information assets.

17.3.9.3 Confidential

Information assets assigned the 'Confidential' classification are those for which disclosure would result in significant negative impact to OIST business, reputation or personnel. This classification includes information assets subject to protection under law or government regulation, including but not limited to personal information such as My Number, credit card and passport information. These assets are to be made accessible only to small restricted groups of users by Information Asset Managers, on a need to know basis. Access is to be regularly audited.

17.3.9.4 Critical

Information assets assigned the 'Critical' classification are those for which disclosure would result in severe negative impact to OIST business, reputation or personnel. Access to 'Critical' information assets shall be granted only to small, tightly restricted groups of authorized users. The strict system access and data access controls must be applied, and access audited regularly.

Information assets can only be assigned the 'Critical' classification upon approval by the Provost or the Secretary General.

### 17.3.10 Protection of Information Assets

In ensuring the basic protection of OIST information assets, users must handle Information Assets in a manner appropriate to the information classification they have been assigned. The security level of the devices used to access information assets and the mode of access must be commensurate with the sensitivity of the asset and conform to OIST information classification and device eligibility criteria.

OIST information assets are to be used for business purposes only, users shall not use OIST information assets for any purpose other than the task for which they are intended. Access to Information Assets must be granted on a "need to know" basis, where required for a user to complete their duties, and in line with business needs.

The protection of personal information is further restricted by the regulations as detailed in. All users which will deal with personal information must familiarize themselves with, and remain abreast of changes to these rules.

### 17.3.11 Information Security

Compliance with information security policy is vital to ensuring the security of OIST information assets, and is the responsibility of all users. In protecting the university

and its information assets users must comply with the rules herein when creating, processing or storing information.

In supporting the CISO to protect the interests of the University, systems administrators shall comply with all rules detailed herein, and comply promptly with directives from the CISO when given.

### 17.3.12 Information Security Incident Response

Information security incidents are defined as a single or series of unwanted events that compromise (or are likely to compromise) the confidentiality, integrity, or availability of OIST Information assets and/or breach OIST rule or Japanese law.

Security Incident Response differs from Data Forensics in that it is triggered by notifications or events, and that only the result of the investigation is disclosed beyond the IT personnel (the Investigator) tasked with investigating it, no data is disclosed. The CISO and the Information Security Committee are responsible for investigating security incidents, and to take all necessary actions in order to protect OIST and its resources and/or to provide information relevant to an investigation. In this regard, the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Director of Institutional Applications and Helpdesk have specific rights and responsibilities.

Any user who becomes aware of an information security incident must immediately contact CIO and CISO via e-mail (cio@oist.jp, ciso@oist.jp), or by phone (see the OIST directory, https://directory.oist.jp).
Please see the Information Security Incident Response Procedures for more details.

### 17.3.13 Data Forensics

Data forensics is the practice of identifying, extracting, and examining data in response to incidents. This may include data held in on IT assets, e-mail, SharePoint, or any other digital repositories.

Data forensics are normally performed after consultation with and consent from the data owner. In cases where the data owner does not consent or where legal or other requirements prevent seeking the consent of the data owner, the approval procedure described below will be used.

As an overarching principle, data forensics should follow PRP1.3.2 Respectful Workplace Policy.

The incidents triggering data forensics, along with the data and IT assets involved, are often sensitive or confidential in nature. The Data Forensics Procedure ensures that all data forensics activities throughout this process are performed in a way that satisfies the objectivity, integrity, and authenticity of the information examined. The procedure requires that appropriate approvals are given, that the privileges of the

parties involved are segregated, and that access to data is limited to only that relevant to the incident.

Request

The data forensics investigation request form (hereinafter referred to as "Request Form" in this section) is completed by the individual (the Investigator) tasked with performing the examination of the data, or responsible for the transfer of custody of the data in cases involving the police, a court or an equivalent authority. The Request Form should include:

- The reasoning behind the request
- The data to be targeted as part of the request
- The duration for which access to the data will be required
- Whether the data owner will be informed and requested to approve the request (normal approval procedure) If not, the reasoning why the data owner cannot be informed or consent cannot be obtained

Approval Procedure

1. Approval by data owner:
   The data owner should always be asked first to approve the access to the data. If the data owner does not agree or cannot be asked, one of the two following approval procedures apply.

2. Simplified approval for the following cases:
   a Internal request by a Compliance Investigatory Committee, Public Research Fund Investigatory Committee or Substantial Investigation Committee (PRP Chapter 23), or other Committees (PRP Chapter 39).
   b External request or order by the police, a court, or an equivalent authority.

The Request Form must be approved by:
- a Vice President, a Dean, the Secretary General, or the Provost;
- the General Counsel; and
- the data owner or the President

Notwithstanding the above, the Investigator cannot serve as one of the approvers mentioned above.

3. Approval for all other cases:
   In all other cases, the Request Form must be approved by both the Approval Committee specified below, the General Counsel, and the President.

The Approval Committee consists of:
a Chair of the Faculty Assembly or their delegate
b Secretary General or their delegate

c A third committee member will be one of the VPs in the University's administration, to be selected in agreement by the two standing committee members, considering the relevant matter and potential conflict of interest. The selection must be made within 24 hours of convening.

In the case that one of the above is the Investigator, that committee member will be replaced by the Provost or by another executive approved by the Chair of the Faculty or their delegate.
The Approval Committee has the authority to deny the request, to approve the request or to approve the request with changes.

Verification
The CIO or delegated representative will receive the request and verify that the appropriate approvals have been provided. They will then appoint a member of the IT Division or the Information Security Section to extract the relevant data. The IT Division or the Information Security Section will have the ability to engage a forensics consultant when deemed necessary.

Extraction
The member of the IT Division, the Information Security Section, or forensics consultant performing the investigation (the Investigator) will extract the requested data to an encrypted, dedicated temporary PC, and give custody to the CIO or a delegated representative.

Access
The CIO or delegated representative will then give custody of the temporary PC and associated access credentials to the Investigator. The Investigator will restrict the data search to material relevant to the request, based, for example, on the subject or the recipient of a message. Privacy of personal communications and the rights of third parties should be respected as much as possible.

Deletion
Once the access duration period has expired, the CIO will ensure the temporary PC is returned and all extracted data is securely erased.

Reporting
The CIO will prepare and send a final report to the President that describes the result of the data forensics activity, and confirms the date of deletion of the data extracted. The CIO will report annually to the Board of Governors, the Executive Committee and the Faculty Assembly the number of requests and approvals in each of the three approval procedures.

Filing
The Request Form will be filed within the Information Security Section, along with the final report.

Responses to IT security incidents are not covered here, and are instead covered under the 17.3.12, Information Security Incident Response in this Chapter.

### 17.3.14 IT Asset Removal

IT Asset Removal is the temporary removal and retention of an IT asset in response to an incident. This may include the removal and retention of laptops, desktops, mobile drives or any other IT asset. IT assets are often critical to business functions, as such their removal is not routine, and must be appropriately requested and approved as described below.

IT assets can be removed and retained upon request by of one of the President, General Counsel, Provost, Secretary General, Dean of Research, or Dean of Faculty Affairs, with the concurrence of the CIO. The CIO will notify the asset owner of the device removal, and delegate a member of IT Division to remove and retain the IT asset within secure IT facilities. The removal of the IT asset may precede the notification to the asset owner where legal or other requirements prevent advance notification.

Access to data held on IT assets, including those that have been removed and retained, is subject to the Data Forensics Procedure.

Responses to IT security incidents are not covered here, and are instead covered under PRP 17.3.12, Information Security Incident Response.

### 17.3.15 Labeling

Information assets must have their document classification clearly marked on the cover page, footer, header or watermark regardless of format. Including but not limited to, printed, handwritten, or electronic documents and records, e-mail contents or subject.
The internal classification may be omitted as it is the default classification.

### 17.3.16 Copying

Users and Document Management Administrators [Link: Chapter 12] shall keep the number of copies of confidential information, in any combinations of media or format, at the minimum required. Where necessary, they shall also keep a record of their distribution. Users shall keep all hard copies or storage media in physically secured storage, such as a locked drawer or filing cabinet. Users shall securely dispose of copies when they are no longer required.
Where information is replicated, the original classification is inherited. Users must evaluate the requirements of integrity and availability against security when creating or replicating information.

### 17.3.17 E-mail

Users are responsible for ensuring that information exchanged via e-mail is protected to a level commensurate with the classification of the information. When

exchanging information with a classification of 'confidential' or higher, strong data encryption must be applied.
The transfer via e-mail of payment information (such as credit card numbers, bank account details), Individual Numbers (My Number), passport information or other personal information is strictly prohibited unless the data is first encrypted.
Refer to the Information Security site for further guidance on managing the risks associated with the use of e-mail.
All administrative employees, and research support employees shall use only the OIST provided e-mail system. The forwarding OIST e-mail to an external e-mail service provider, or access to OIST e-mail servers from external providers is not permitted.

### 17.3.18 Prevention of information leakage or manipulation in transit

Users shall apply security controls when transmitting data of 'confidential' or higher classification to external parties.

- Such data must be encrypted prior to transmission
- Encrypted data and password should be transmitted separately, ideally via different mechanisms.
- The use of multiple entity protection is encouraged.

### 17.3.19 Use of removable media

The following restrictions apply to removable media devices, including but not limited to USB thumb drives, mobile hard drives, SD cards and any other transportable or mobile storage technologies:

- Within the administration, the use of removable media is prohibited, repositories provided by IT Division are to be used. Contact IT Division to seek exception from the CISO or CIO.
- Within research units, the use of removable media to store 'Confidential' and 'Critical' information is at the discretion of the faculty.

Refer Information Security site for further guidance on managing the risks associated with the use of removable media. (Information Security Site)

### 17.3.20 Remote access

When accessing OIST IT resources from outside the OIST network, users must first obtain advance permission from IT Division, and access resources only via approved OIST IT remote access services (VPN, SSH, etc.)

The use of any non-OIST managed remote access software or services, such as Team viewer, to provide external access to OIST IT resources is prohibited. Exceptions may be granted by the CIO or CISO where network security has been enhanced, users must contact IT Division to request an exception.

### 17.3.21 Information disposal

Users must securely erase 'internal' or higher classified information promptly in non-recoverable manner when they are no longer required. Users must physically destroy all hard copy of confidential documents in non-recoverable manner prior to disposal. Users shall escalate to IT Division as required [Link: 17.5.1].

### 17.3.22 IT Asset Security

All users are responsible for preventing the theft of IT assets. Users shall ensure following controls in order to prevent theft of, or unauthorized access to IT Assets.

- IT Assets except mobile devices shall be locked with security wire in all publically accessible locations, or where the asset has accessed data of classification of 'Confidential' or above
- IT Assets must be securely stored in locked drawers or cabinets when not in use
- Screen lock functions must be configured to activate automatically after no longer than 5 minutes

### 17.3.23 Protection against malicious software

Users are responsible for ensuring that any IT asset they manage have:

- Latest software patches and updates applied
- Anti-virus or other applicable anti-malicious software installed and up to date
- Real-time inspection of files for malicious software is enable Potentially malicious files quarantined when detected
- A full scan of the files to detect malicious software run periodically
- All data or software received from external parties scanned before opening or importing

Users must remain abreast of the latest security updates from IT, and make efforts to prevent malicious software infection

### 17.3.24 Mitigation of threats to IT Services

OIST is under constant attack from external parties seeking to access and exploit its IT Resources. In protecting OIST and its users, IT Division and systems administrators shall conform to the following requirements.

#### 17.3.24.1 Software vulnerability management

System administrators shall ensure patches or workarounds are in place for any published vulnerabilities prior to production use of any software. Once a system has moved to production operation, system administrators shall remain appraised of updates and patches to systems, and apply them in a timely fashion, accounting for potential impact to the system and its users. Where a vulnerability which may result in the compromise of OIST information assets is detected, the system

administrator shall immediately contact the CIO and CISO and take appropriate action to protect OIST information assets.

17.3.24.2 Measures to limit malicious software

System administrators shall install anti-malware software into servers or other devices that supports such software. The system administrator shall monitor status of anti-malware software and take any action necessary. The system administrator shall keep anti-malware software and its definition files up to date. Only system administrators shall have the escalated privileges required to change the configuration of anti-malware software, and shall not grant such privilege to other users. The system administrator shall configure anti-malware software to scan to the system periodically.

### 17.3.25 Intrusion prevention

The system administrators shall implement the following controls in order to prevent intrusion into servers and systems;

- Delete or turn off unnecessary services
- Prevent the execution of unknown or unauthorized programs or code
- Ensure firewall configurations are created and updated such as to allow only the communication channels required for the operation of the system or software

The system administrator shall implement the following controls in order to prevent intrusion via removal media (where the use of such devices is permitted) ;

- Disable all unnecessary USB ports or physical connections to the server or device
- Scan removable media using anti-malware software upon connection

### 17.3.26 Training

17.3.26.1 User training

Supervisors are responsible for ensuring that a user is properly trained with regard to information security prior to commencing work, and is to ensure that the user conducts themselves accordingly.

17.3.26.2 System Administrators Training

System Administrators must be fully trained in all aspects of system security prior to being granted escalated privileges to OIST systems.

### 17.3.27 Web presence

17.3.27.1 Domain name management

IT Division manages the oist.jp domain on behalf of the Communications and Public Relations division.

Research unit websites shall be located within the unit.oist.jp domain or other subdomain and under the control of IT Division. This rule is in place to allow clear

differentiation between the core university web presence and that of the research units or projects.

17.3.27.2 Internet domain name per purpose

Research projects which require a URL which lies entirely outside of the OIST domain, shall request IT Division to register the external domain name and to create the virtual machine to house the site. This request shall be approved by the CIO, and the Dean of Faculty Affairs.

These domains shall normally be restricted to .org or .net (non-profit) extensions, other domains shall require consultation with and approval by the CIO. All units are required to keep their OIST unit (groups) site up to date, the creation of any websites for the promotion of the unit itself outside of this space is discouraged.

### 17.3.28 Operation and Management

17.3.28.1 Business continuity planning

Information asset managers and IT Division shall develop business continuity plans, ensuring the availability of OIST information assets and resources. Business continuity plans shall be tested at least annually to validate their effectiveness, and to ensure staff are appropriately trained in its execution.

17.3.28.2 Backup

Information Asset Managers and IT Division shall ensure that information assets are backed up to a frequency, and to a level of redundancy, commensurate to the value of the assets. Information Asset Managers shall identify the retention period of information assets and manage them.

Restore tests are to be conducted annually, or more frequently for 'Critical' or rapidly evolving information assets.

Information Asset Managers shall request IT Division delete, revoke or physically destroy backup data for assets which have exceeded their retention period, or no are longer required.

17.3.28.3 Change management

Change Management is a process that ensures that any change made to OIST IT Resources is documented, reviewed and approved. It encompasses both larger planned changes such as projects and smaller reactive changes such as software patches and unscheduled server maintenance. Change management processes and procedures must be in place, documented and implemented for all OIST IT Resources. Management responsibilities and procedures will be defined to ensure satisfactory control of all changes to equipment, software, or procedures. These procedures will be defined in the SLA.

### 17.3.29 Access to OIST IT facilities

Access to OIST IT facilities, including server rooms and network and communication spaces, is restricted. All access to these facilities is subject to authorization and authentication, access must be approved by the CIO or CISO.

Access for the purposes of site-tours should be coordinated through the CIO Office.

#### 17.3.30 Hosting of hardware in OIST IT facilities

Any party at OIST wishing to purchase and/or house hardware (including servers and storage) into OIST IT facilities must consult with IT Division. Failure to do so will likely result in the hardware being ineligible to be housed; IT Division reserves the right to refuse to house any hardware it does not deem appropriate or safe to house in OIST facilities. The hardware must further confirm to OIST server hardware requirements, the basic requirements for server hardware are specified at PRP 17.5.6.

#### 17.3.31 Logging and monitoring

IT Division shall as a matter of course collect and analyze logging information from IT resources in order to detect intrusion or misuse. IT Division retains the right to access any and all logging information generated by any IT resource for this purpose. In complying with legal requirements and contractual obligations, IT Division shall also retain audit logs covering user activity, security events and any other relevant information. This information is classified as 'confidential' and access restricted to appropriate members of IT Division accordingly.

#### 17.3.32 Further Policies Rules and Procedures

Faculty or Vice Presidents within the University may impose additional rules and procedures upon the use of OIST information assets. Such additional rules and procedures must be consistent with this Chapter; but they may provide additional detail or greater restrictions; they may not reduce restrictions.

Students should refer to the Chapter 5 "Graduate School Handbook" in addition to familiarizing themselves with this chapter.

### 17.4 Right and Responsibilities

#### 17.4.1 The University

The University owns and controls all its information assets. Though the University takes reasonable security measures to protect the security of its IT resources, the University does not guarantee absolute security nor privacy. The University has the right to monitor any and all IT Resources and their usage, including e-mail, without limitation. The University is responsible for taking any measures necessary to ensure the security and integrity of its IT Resources. When it becomes aware of violations of policy or Japanese law, either through routine system administration activities or via incident notification, it is the responsibility of the University to investigate as needed or directed, and to take all necessary actions in order to protect its resources and/or to provide information relevant to an investigation.

In this regard, the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Director of Institutional Applications and Helpdesk have specific rights and responsibilities.

### 17.4.2 User's rights and responsibilities

Users are granted access to IT resources in order to conduct University business. In using these resources, users agree to abide by all relevant University policies, rules, procedures and applicable law. Users must acknowledge this understanding by reading and signing the OIST Graduate University Acceptable Use Policy, via physical signature or digital equivalent.

### 17.4.3 Faculty

Faculty members serve as Information Asset Manager for information assets within their purview, and may delegate the Information Asset Administrator role to a unit member. In managing research Information Assets, Faculty will give due consideration to contractual requirements, such as research agreements with other Universities or companies.

Faculty are responsible for ensuring that users under their supervision are trained in all relevant IT policy, rules and procedures as well as applicable law prior to commencing work.

### 17.4.4 Vice Presidents, Senior Managers and Managers

Vice-Presidents are responsible for nominating Information Asset Managers to manage information Assets within their remit.

Vice-Presidents, Senior Managers and Managers are responsible for ensuring that users under their supervision are trained in all relevant IT policy, rules and procedures as well as applicable law prior to commencing work.

### 17.4.5 Chief Information Officer (CIO)

The CIO has the following general accountability and responsibilities with regard to University IT:

- Establishing a strategic plan for University Information Technology
- Overseeing the development, installation and maintenance of IT systems
- Establishing and disseminate enforceable rules regarding access to and acceptable use of Information Assets
- Establishing reasonable security policies and measures to protect data and systems
- Monitoring and managing system resource usage
- Investigating problems and alleged violations of University policy, and reporting violations to the President

- Designating a Chief Information Security Manager (CISO)

### 17.4.6 Chief Information Security Officer (CISO)

The CISO has overall responsibility for ensuring the security of the University, including:

- Developing security processes and procedures
- Conducting information security incident response, reporting results to the CIO
- Developing, installing and operating IT security monitoring systems

### 17.4.7 Information Security Committee

Information Security Committee shall review the information security programs of the university and assess information security risks in order to protect OIST information assets. The committee shall also support the CISO in security incident response. Committee regulations shall be established separately.

### 17.4.8 Information Security Auditor

Information Security Auditor shall plan and conduct annual information security audit and supervise the audit. The Chief Internal Audit Officer (CIAO) shall serve as the Information Security Auditor.

### 17.4.9 Information Asset Manager

Information Asset Managers are accountable for defining the classification level of, authorizing access to, and ensuring an appropriate permission scheme for, the information assets within their remit, in accordance to any and all relevant laws, rules and regulations. In most cases, Information Asset Manager is the head of a research unit or administrative division handling the information asset.

The Information Asset Manager may designate an Information Asset Administrator to manage information assets, but accountability remains with the Information Asset Manager.

### 17.4.10 Information Asset Administrator

Information Asset Administrators are responsible for ensuring appropriate handing of OIST information assets.

### 17.4.11 Privileged users and System Administrators

All users granted escalated privileges, including System Administrators, are responsible for the application of this and related policies to the IT resources in their care, under the direction of system owners and Information Asset Managers. Beyond the OIST Acceptable Use Policy, these users must also read and sign the System Administrators Code of Conduct.

### 17.4.12 Third-party users

OIST expects all partners, consultants and vendors agree to, and abide by all relevant University policies, rules and procedures, as well as all applicable law. If information assets or resources above a "Public" classification are to be accessed or shared with these third parties, they shall be bound by contract to abide by OIST Acceptable Use Policy as well as a suitably drafted non-disclosure agreement.

#### 17.4.13 System Developers and Integrators

System Developers and Integrators are responsible for the application of this and related policies to all IT resources in their purview. If information assets or resources above a public classification are to be accessed or shared with these third parties, they shall be bound by contract to abide by OIST Acceptable Use Policy as well as a suitably drafted non-disclosure agreement.

### 17.5 Procedures

For details on the IT procedures and Information Security, please see the Service Portal Website
https://oist.service-now.com/sp

#### 17.5.1 General IT request process

Any user wishing to contact OIST IT can do so via;

- E-mail: it-help@oist.jp
- Web request form: https://oist.service-now.com/sp
- In person: Lab 2 Level B (mountain side)

#### 17.5.2 Purchasing or upgrading an IT asset within the administration

The purchase or upgrade of an IT assets within the administration is to be performed via IT Division. The catalog of standard devices is as listed on the Service Portal Website. Purchasing requires the approval of the section manager, once obtained staff should contact IT [Link: 17.5.1]. Non-standard devices are permitted by exception from the CIO or Director of Institutional Applications and Helpdesk

#### 17.5.3 Purchasing or upgrading an IT asset within research units

The catalog of standard hardware is provided on the Service Portal Website. These devices are tested and well supported in the OIST environment. If researchers wish to purchase any item on the catalog, they can contact IT Division via the process described in PRP 17.5.1 to request a quote.

If researchers wish to purchase any devices not on the catalog, they are strongly encouraged to contact IT Division first to ensure that the device will be compatible with OIST systems. IT Division also has a strong knowledge of local vendors and is better placed to negotiate.

In the case that IT assets are to be part of or attached to research equipment, guidelines regarding the specification of these assets are defined here:

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0012667

#### 17.5.4 Offsite Usage Authorization

https://oist.service-now.com/sp?id=sc_cat_item&sys_id=ea1eea70db8aeb004a187b088c9619f2&sysparm_category=59d4b9b2db65e380d7c7e5951b961906

#### 17.5.5 How to re-allocate or relinquish an IT asset

https://oist.service-now.com/sp?id=sc_cat_item_guide&sys_id=87501059db2ce3406885f00ebf961971&sysparm_category=ef2e888edb47df004a187b088c96199a

#### 17.5.6 Hosting devices in IT facilities

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0011735

#### 17.5.7 Specification process for enterprise applications

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013669

#### 17.5.8 Information Security Incident Response

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013330
https://groups.oist.jp/it/info-sec-incident-response

#### 17.5.9 Email & Online Communication Code of Practice

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013662

### 17.6 Forms

#### 17.6.1 OIST Graduate University Acceptable Use Policy

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0011736
https://groups.oist.jp/it/it-aup

#### 17.6.2 System Administrators Code of Conduct

https://oist.service-now.com/sp?id=kb_article_view&sysparm_article=KB0013709
https://groups.oist.jp/it/info-sec-aua

### 17.7 Contacts

Policy Owner: Chief Information Officer

### 17.8 Definitions

### 17.8.1 Information Technology Resources (IT Resources)

The University defines its IT Resources as comprising of the set of all Information assets, and Information Technology Assets (IT Assets).

### 17.8.2 Information Assets

The University defines its Information Assets as comprising of all University information; including but not limited to all research and administrative, data, files, workflows and mechanisms for managing University information regardless of media format. This broad definition encompasses special categories of information assets for which further rules and procedures apply, such as Corporate Documents, and Personal Information.

### 17.8.3 Information Technology Assets (IT Assets)

The University defines IT Assets as all computer, communication devices and other technologies which access, store or transmit digital University Information; including but not limited to electronic networks, systems, cloud services, computers, devices, telephones and software, whether wholly owned by the university or otherwise.

### 17.8.4 Devices

Device is a synonym for Information Technology Assets.

### 17.8.5 Information Technology Service Management (ITSM)

Information Technology Service Management (ITSM) is a set of practices that focuses on aligning IT services with the needs of business.

### 17.8.6 Service Level Agreement (SLA)

A Service Level Agreement (SLA) is a document defined in the ITSM standard. This document describes the level of service expected of IT Division by users, and lays out the metrics by which that service will be measured. https://groups.oist.jp/it/it-service-level-agreement

### 17.8.7 Information Security

The underlying principles of information security are described on the OIST Information Security Website.

### 17.8.8 Legislation Relevant to Information Security

The following legislation is relevant to Information Security at OIST.

- Act on Prohibition of Unauthorized Computer Access
- Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc.
- Act on Access to Information Held by Incorporated Administrative Agencies, etc.
- Act on Electronic Signatures and Certification Business (Electronic Signatures Act)

- Copyright Act
- Unfair Competition Prevention Act

### 17.8.9 Information classification and device eligibility

https://groups.oist.jp/it/info-sec-classification

### 17.8.10 Information System (System)

An information system is a system composed of people and computers that processes or interprets information. In the case of OIST, information systems are systems that process, transmit or store OIST information assets. This includes but is not limited to systems developed, purchased or outsourced.

### 17.8.11 Users

Any individual or entity granted access to OIST IT Resources to a level above that available to the general public.

### 17.8.12 Information Asset Manager

Individuals accountable for defining the classification level, authorizing access to, and ensuring an appropriate permission scheme for the information assets, in accordance to any and all relevant laws, rules and regulations.

### 17.8.13 Information Asset Administrator

Individuals tasked with ensuring appropriate handing of OIST information assets.

### 17.8.14 Escalated Privileges

Privileges which allow users access to information assets or IT resources to a level beyond that normally permitted.

### 17.8.15 Privileged users

Users granted escalated privileges.

### 17.8.16 System Administrator

A subset of privileged users, possessing administration rights to systems or services.

### 17.8.17 Identity Management System (IDM)

The OIST Identity Management System (IDM) handles enterprise or cross-network identity management. The system controls OIST authentication and authorization systems, facilitating appropriate access schemes to information assets.

### 17.8.18 Server

A system that responds to requests across a computer network to provide, or help to provide, a service.

### 17.8.19 Storage media

Storage media is a device or tangible object for storing digital information, including hard drives, USB memory, DVD's etc.

### 17.8.20 Removable media
Storage media designed to portable.

### 17.8.21 Securely erase
To render all data on a storage media unreadable in an unrecoverable fashion.

### 17.8.22 Outsourcing
Provisioning services or systems under contract from a supplier external to the University.

### 17.8.23 Entity
A person, process, client, or server accessing OIST IT systems.

### 17.8.24 Entity Authentication
The process by which one entity is assured of the second.

### 17.8.25 Identification
Specification of the entity accessing the system.

### 17.8.26 Access control
The limitation of access to information resources to only permitted entities.

### 17.8.27 Access right management
To manage the authorization information in accounts and access control.

### 17.8.28 Account
Any entity registered into the OIST IDM.

### 17.8.29 Encryption
The process of encoding information assets in such a way that only authorized entities can read it.

### 17.8.30 Malicious program (Malware)
Malware is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

### 17.8.31 Anti-malware definition file
Data which is referred by Anti-Malware software to determine the malicious program.

### 17.8.32 CMDB

The OIST configuration management database (CMDB) is a repository that stores information regarding IT assets, as well as descriptive relationships between them.

### 17.8.33 Software catalog

https://groups.oist.jp/ja/it/oist-software

### 17.8.34 Disaster recovery and Business continuity planning

Disaster recovery (DR) involves a set of policies, procedures, systems and organization to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Business continuity plan (BCP) is a plan to continue operations if a place of business is affected by different levels of disaster which can be localized short term disasters, to days long building wide problems, to a permanent loss of a building.

### 17.8.35 Information security incident

Information security incidents are defined as a single or series of unwanted events that compromise (or are likely to compromise) the confidentiality, integrity or availability of OIST information assets and/or breach OIST policy or Japanese law. A compromise is an incident where the security of a system or its information was successfully harmed.

Examples of information security incidents include:

- Data loss due to any cause including operation error such as personal data being e-mailed to the wrong recipient
- Unauthorized use of a system for the processing or storage of data
- Noncompliance with information security and acceptable use policies
- Theft or other loss of a laptop, desktop, PDA, or other device that stores the University information, whether or not the device is owned by the University
- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Malfunctions of software or hardware

### 17.8.36 An advanced persistent threat (APT)

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT processes require a high degree of covertness over a long period of time. The advanced process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The persistent process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The threat process indicates human involvement in orchestrating the attack.