Chapter 17. Information Technology and Security

17.1 Policy
Computers, networks and electronic information systems are essential resources for accomplishing the OIST Graduate University (the University)’s mission [link: 1.2] of graduate education, research in science and technology, outreach to Okinawan society, and all associated administrative and business transactions. The University grants members of the University community shared access to these resources in support of accomplishing the University's mission. These resources are a valuable asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate educational, business, and cultural activities. All those authorized to access these resources [link: 17.8.5] are required to use them in an effective, efficient, prudent and responsible manner (Chapter 21.3.2 [link: 21.3.2]).

The University’s information technology (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.

Although the University takes reasonable security measures to protect the security of its computing resources and accounts assigned to individuals, the University does not guarantee absolute security and privacy.

17.2 General Considerations

17.2.1 The University owns and controls the University IT in all its forms (Chapter 17.4.5 [link: 17.4.5]).

17.2.1.1. The University has the right to monitor any and all IT use, including email, without limitation. Such monitoring is ordinarily limited to carrying out routine security and network maintenance. However, authorized individuals within the University may be directed by the Chief Information Officer (CIO) [link: 17.4.7] to monitor more extensively equipment, systems, and network traffic (including email) if reasonable grounds exist to suspect that the integrity of computers, networks, or data is threatened, or if
reasonable grounds exist to believe that electronic communications may be being used in a manner not compliant with University policies or Japanese law. Additionally, IT equipment may be confiscated, without notice, for forensic review upon direction from the General Counsel and/ or the Vice President for Administrative Compliance with the concurrence of the President and the CIO (Chapter 17.3.7 [link: 17.3.7.3]).

17.2.2 All users, including guests, are subject to the requirements set out in “Users’ Rights and Responsibilities” [link: 17.4.4], which outlines obligations and constraints related to personal communication, privacy, and security as well as the consequences for violations.

17.2.3 Use of University IT resources, other than those available to the general public (for example, web access to public-facing websites), requires reading and signing of the University’s Use Agreement [link: 17.6.1] as well as authentication that identifies the specific user.

17.2.3.1 Exceptions to the authentication requirement may be acceptable in certain circumstances (for example, guest logins for conference delegates or the use of guest logins in libraries and "kiosk" settings), provided that appropriate measures are taken to manage the risk of misuse or security compromise.

17.2.3.2 Physical access to the University’s IT facilities by guests, students and University personnel not in the Information Service section nor the Scientific Computing & Data Analysis requires approval by and coordination with the CIO’s office (Chapter 17.5.11 [link: 17.5.11]).

17.2.3.3 Hosting equipment within University IT requires close coordination and planning with the CIO’s office (Chapter 17.5.2 [link: 17.5.2]).

17.2.4 The University assigns responsibility for protecting its resources and data to system administrators and data custodians, who are required to treat the contents of individually assigned accounts and personal communications as private. These individuals do not examine or disclose personal communication except as required for system maintenance including security measures, or if there exists reason to believe an individual is violating the law or University policy, or as permitted by applicable policy
or law.

17.2.5 Other standards and rules developed by the Vice President for Communication and Public Relations [link: 16.3] apply to use of University IT with regard to email, websites, and social media; compliance with those standards and rules is mandatory.

17.2.6 Students should refer to the Graduate School Handbook [link: 5] in addition to familiarizing themselves with this chapter.

17.2.7 Individual units within the University may impose additional conditions of use for resources or facilities under their control. Such additional conditions must be consistent with this overall policy. They may provide additional detail, guidelines, or greater restrictions. They may not provide lesser restrictions.

17.3 Rules

17.3.1 Access to and Use of Computing Resources.
Every person wishing to use any University IT must read and acknowledge by signature (or digital equivalent) the OIST Graduate University IT Resources Use Agreement [link: 17.6.1] and must read and sign Users’ Rights and Responsibilities [link: 17.4.4] before access to the University's IT resources can be authorized.

17.3.1.1 Access to secure areas, including computer rooms, network equipment rooms and any associated service facilities, is restricted to authorized users (Chapter 17.5.11[link: 17.5.11]).

17.3.1.1.1 Physical access to University IT Facilities ordinarily must be limited to those carrying out preplanned or remedial activity, such as implementation, maintenance or incident-related work.

17.3.1.2 Access for other purposes, such as site visits, must be prearranged through the CIO’s office.

17.3.1.2 Use of and access to IT equipment and facilities is subject to authentication and authorization.

17.3.1.2.1 Records of authorization and access must be kept in
a manner that preserves accountability.

17.3.1.3 Required IT Training. All aspects of IT security, including confidentiality and procedures relating to system access, must be explained to students, employees, and other users.

17.3.1.3.1 Students. IT training of students is the responsibility of the Dean of the Graduate School (Chapter 5 [link: 5]).

17.3.1.3.2 Employees. On commencement of and during their employment, each employee must be specifically informed of the duty to maintain the confidentiality of sensitive or confidential information to which the employee may have access during the course of their employment.

17.3.1.3.2.1 Staff must be informed that they may not seek access to data that is not required as part of their duties.

17.3.1.3.2.2 When employees cease employment or change positions within the University, their unit must effect any needed changes to roles and access privileges in the appropriate system and according to established business processes.

17.3.1.3.2.3 When privileged users [link: 17.3.6] change roles or leave the University, their privileged access must be disabled before or at the time of separation.

17.3.1.3.3 System Administrators must be fully trained in all aspects of system security prior to supporting these systems.

17.3.2 Physical Protection of Computing Resources. All University network cabling, conduits and physical communication channels must be physically secured, sequestered, and protected to the extent reasonably possible, and in accordance with industry best practices, to prevent damage or unauthorized access.

17.3.2.1 IT infrastructure must be located in secure areas.
17.3.2.2 Appropriate physical security measures must be taken to protect desktop computers and related devices.

17.3.2.3 Guest access to University IT resources is contingent upon reading the Users’ Rights and Responsibilities [link: 17.4.4] and reading and signing the OIST Graduate University IT Resources Use Agreement [link: 17.6.1].

17.3.3 Password Protection of Computing Resources and Protected Information

17.3.3.1 End-user computers and other end-user network devices must be configured in such a manner that a password or other authentication method is required to gain access.

17.3.3.1.1 When unattended, such devices must be left in a state where a password or other authentication method is required to gain access.

17.3.3.2 Passwords must be "good passwords":
- at least 8 characters long,
- containing letters and numbers,
- easy to remember but difficult to guess or crack, and
- not dictionary words.

17.3.3.3 Users must exercise due care to keep their password secret. Recklessness or negligence in this duty of care may lead to disciplinary action or other consequences.

17.3.3.3.1 Password breaches must be immediately reported if the user has any reason to suspect that the secrecy of a password has been compromised.

17.3.3.3.2 Users must never provide their password, or any other authentication data of a kind useful in identity theft or in gaining unauthorized access, by email.

17.3.3.3.2.1 Inappropriate IT-related activity carried out using a password or other form of authentication will be attributed to the User to whom that password or
authentication belongs.

17.3.3.4 Systems must enforce rules intended to make passwords as strong as they can be.

17.3.3.4.1 Systems must require users to change their password at appropriate intervals determined by the relevant system custodian.

17.3.3.4.2 Systems must restrict password re-use.

17.3.3.4.3 System-specific rules are determined by the relevant system custodian.

17.3.3.5 Providers must never request passwords, or any other authentication data of a kind useful in identity theft or in gaining unauthorized access, by email.

17.3.4 Personal Communications.
Users of the University IT resources are responsible for the content of their personal communications. Compliance with the policies, rules, procedures and standards owned by the Vice President for Communication and Public Relations [link: 16.3] is mandatory. The University accepts no responsibility or liability for unauthorized use of its IT communication resources or for use not in compliance with University policies and Japanese law.

17.3.5 Maintaining and Securing “Protected Information”.
Information that is personal, private, sensitive, confidential, or otherwise subject to disclosure restrictions is characterized for purposes of this Chapter as “Protected Information”. Users are bound by Japanese law and by University rules concerning use and disclosure of any information, but especially protected information.

17.3.5.1 Any data stored on desktops, laptops and other personal or mobile devices is the responsibility of the user: the user is the custodian for this data.

17.3.5.1.1 It is the custodian’s responsibility to establish authentication and authorization guidelines for data.

17.3.5.1.1.1 Any third party receiving protected
information must be authorized to do so.

17.3.5.1.1.2 Any third party receiving protected information, or their organization, must have adopted IT security measures which protect the confidentiality and integrity of that data.

17.3.5.2 Users may access only accounts, files, and data that are their own, that are publicly available, or to which they have been given authorized access.

17.3.5.2.1 Users may not seek access to data that is not required as part of their duties

17.3.5.2.1.1 University information may be used only for tasks related to job responsibilities and not for personal purposes.

17.3.5.3 Users are the custodians of, and must secure, information in their possession.

17.3.5.3.1 Special care must be taken with protected information, for which the use of encrypted containers is recommended.

17.3.5.3.1.1 Maintain the confidentiality of information classified as private, personal, or confidential.

17.3.5.3.1.2 Never disclose information to which you have access, but for which you do not have ownership, authority, or permission to disclose.

17.3.5.3.1.3 Consistently back up all data.

17.3.5.4 If protected information must be communicated online, the information and credentials used must be encrypted by a sufficiently strong encryption method.

17.3.5.5 Protected University information is not to be stored on third-party facilities without approval of the CIO.
17.3.6 **Privileged Users.**
Certain users have high-level access rights, enabling them to access any data stored on the University’s IT systems. These people are privileged users. Privileged users must abide by the University’s Code of Conduct [link: 1]. Privileged users found to have breached the Code of Conduct may be subject to disciplinary action or other consequences.

17.3.6.1 Security controls must be implemented to prevent, detect or correct abuse of privileged accounts.

17.3.6.2 Use of two-factor authentication is desirable in remote privileged access.

17.3.6.3 Representatives of external organizations whose IT security policies do not meet or exceed the standard of this policy must not be allowed privileged access to University IT facilities.

17.3.6.4 Factory-supplied default passwords must be changed as early as possible in the provisioning process.

17.3.7 **Information Security and Cyber security Program.**
The University must protect its data against unauthorized access and, in a related and coordinated manner, it must maintain a robust and effective cyber security program to protect data and systems in networks that are connected to the Internet. Additionally, Users must follow the appropriate security procedures [link: 17.5] to assist in keeping systems and accounts secure.

17.3.7.1 The CIO [link: 17.4.7] has primary responsibility for the establishment and operation of the University’s Information Security and Cyber Security Programs.

17.3.7.2 Security Incident Response. Employees authorized by the CIO will investigate IT security incidents and obtain such information as they reasonably consider necessary in such manner as they reasonably consider appropriate.

17.3.7.2.1 All users are required to co-operate in such investigations and to comply with reasonable requests for information made in the course of those investigations.
17.3.7.2.2 Investigating officers are required to maintain confidentiality of information obtained in the course of investigations.

17.3.7.3 In order to protect the integrity, security, or continued operation of its computers and networks or to protect itself from liability, officers authorized by the CIO (who must first obtain the concurrence of the President) may do any or all of the following:

17.3.7.3.1 confiscate University computer equipment,

17.3.7.3.2 temporarily remove material from University websites,

17.3.7.3.3 disable or close any University-provided account,

17.3.7.3.4 shut down or disable access to any server or service,

17.3.7.3.5 expand monitoring of network traffic,

and/or

17.3.7.3.6 temporarily deny access to all networks and computers.

17.3.7.4 Alleged policy violations by the University employees, students, or other users will be referred to the President of the University.

17.3.7.4.1 The University may also refer suspected violations of law to appropriate law enforcement agencies.

17.3.7.4.2 Users other than University staff and students, and users of facilities other than University facilities, are subject to the disciplinary arrangements of the relevant external organization, although suspected violations of law may be referred to the relevant law enforcement agencies.

17.3.7.5 Consequences for Misuse of University Resources
Depending on the nature, willfulness, and severity of the offense, violations of information security and cyber security requirements may result in loss of access privileges, University disciplinary action
up to and including termination, and/or criminal prosecution. (see also Misconduct & Whistleblower Protection [link: 23])

17.3.8 **Specification formulation of Enterprise Systems**

17.3.8.1 Enterprise Systems at the University

An enterprise system is defined as any system or software which is intended for the University business, and is to be used by more than 10 users or crosses a section boundary in usage. The functionality and quality of these systems can have substantial impact on the University business productivity, and so the definition and specification of these systems must be conducted with due diligence. Prior to the procurement process, consideration must be given to as to;

- The function and effect of the system across the entire university, not just within the section or area seeking it
- How the system will integrate with other the University systems
- If the system will meet the users requirements and expectations
- If the system is actually required
- What options exist to provide the function of the system
- If business processes need to be modified to improve the function of the system
- That the University has the facilities or capacities required to house and maintain the system
- Other items regarding the systems as necessary

To ensure adequate consultation and consideration is given to new system, the definition and specification creation process is to be treated as a project. The Project will be undertaken by a working group, chaired by a Project Manager. The role of Project Manager will be assumed by the manager from the section or area seeking to acquire the system. The project manager is responsible for selecting working group members, ensuring that the following procedures are followed, and that the required documents and evidence exists prior to the start of the procurement process.

The Working Group is to consist of:
No less than 1 faculty member
• No less than 2 key users (from outside the section procuring the product)
• The CIO or assigned representative
• No more than 3 members from the section or division procuring the product
• No more than 8 voting members
• No more than 12 members in total, including the secretariat

Note: The Dean of Research can modify membership of the Working Group as required by the evolving needs of the Project or system.

These members are to be selected based on their expertise in the field that the new system will cover, and their investment in the successful function of the system. The Dean of Research will approve the membership of the Working Group, and adjust as necessary.

The Working Group will conduct the project through the following stages of definition and specification process, prior to the procurement process.

17.3.8.2 Definition and Specification Project Process

17.3.8.2.1 Needs Analysis
The Project shall begin with a needs analysis. Here the Working Group is to meet and discuss:
• What are the business requirements the University will place on the system
• The legal requirements on the system and the processes the University must use to meet them
  ➢ This is key to educating users, and preventing functionality made mandatory by legal requirements being viewed as unnecessary complexity of the system
by users

- What alternatives exist
- Are current the University business practices best aligned to work with this kind of system
- Whether the implementation of this system should be phased or staged
- How this system will interface to any or all other the University systems

The key outcome of this phase is the refinement of the system requirements that will result in a system which is simple to use, maintainable and easy to support as possible.

This step will consist of at least one meeting; the Project Manager shall ensure that meeting minutes are recorded. The meeting can be either face to face, or via teleconference.

17.3.8.2.2 Demonstration (optional)

- The Working Group will attend presentations on candidate systems
- The Working Group will then informally discuss the systems presented

17.3.8.2.3 User Feedback

- The Working Group will solicit user feedback
- This stage may be combined with the demonstration phase

The Project Manager is to keep record of user feedback, and detail who was consulted. The user feedback sessions can either be a presentation style meeting, or a small group session.

17.3.8.2.4 Specification

- The specification is to be drafted by the Project Manager, in consultation with the Working Group members.
- The Working Group then meets to review the specification
- Any changes or alterations are then to be made and another meeting held
- All members must vote to pass the specification before it
proceed to the procurement phase

17.3.8.2.5 Procurement
• The Working Group will propose appropriate type of procurement to the Procurement and Supplies Section according to the nature of the Project or candidate system.

17.3.8.2.6 Requirements
• The specification cannot be accepted procurement process until the following documentation is submitted:
  ➢ Meeting minutes from the needs analysis meetings
  ➢ User feedback and a list of users consulted
  ➢ Approval(KESSAI) of the specification by all Working Group members

17.3.8.2.7 Working Group in the Procurement Phase
As part of the move to the procurement phase, the Working group move to become members of the selection panel for the product, with the remainder of the members and structure determined by the relevant procurement rules and procedures as detailed in the chapter 28 [link: ].

17.4 Responsibilities

17.4.1 Employees and Students.
Virtually all students and all employees are Users. As such, they must understand and comply with “Users’ Rights and Responsibilities” [link: 17.4.4], which outlines constraints related to personal communication, privacy, and security as well as consequences of violations, and they must read and sign the OIST Graduate University IT Resources Use Agreement [link: 17.6.1].

17.4.1.1 All employees and all students must be trained in the use of IT and their duties with regard to IT; however, IT training for students is the responsibility of the Dean of the Graduate School (Graduate School handbook [link: 5]).

17.4.2 Guests
All guests granted access to University IT resources must read, understand, and comply with “Users’ Rights and Responsibilities” [link: 17.4.4], must sign the OIST Graduate University IT Resources Use Agreement [link:
17.6.1, and must be given training in the use of IT by their host.

17.4.3 Supervisors and Managers.
Supervisors and managers must instruct their employees and guests concerning the requirements set forth in “Users' Rights and Responsibilities” [link: 17.4.4], must train their employees and guest in the use of University IT, and must ensure that their employees and guest read and sign the OIST Graduate University IT Resources Use Agreement [link: 17.6.1].

17.4.4 Users’ Rights and Responsibilities.
Members of the University community are granted access to IT resources in order to facilitate their University-related academic, research, and job activities. By using these resources, users agree to abide by all relevant University policies, rules and procedures, as well as all applicable law. These include but are not limited to University policies, rules, and procedures related to harassment, plagiarism, commercial use, security, privacy rights, and unethical conduct, as well as laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and protection of privacy.

17.4.4.1 Guests who are granted access to IT resources must abide by all relevant University policies, as well as all applicable laws. These include but are not limited to University policies, rules, and procedures related to harassment, plagiarism, commercial use, security, and unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws.

17.4.4.2 All Users, including Guests, must review, understand, and comply with all policies, rules, procedures and laws related to access, acceptable use, and security of University IT resources, and they must report possible policy violations to the appropriate entities [link: 17.7].

17.4.5 The University's Rights and Responsibilities.
As owner of the computers and networks that comprise the University's IT infrastructure, the University owns all data that resides on its systems and networks, and is responsible for taking necessary measures to ensure the security of its systems, data, and user's accounts. The University does not ensure absolute privacy or security. When it becomes aware of violations, either through routine system administration activities or from a complaint, it is the University's responsibility to investigate as needed or directed, and
to take all necessary actions, including but not limited to monitoring of network traffic, to protect its resources and/or to provide information relevant to an investigation.

17.4.6 University's Information Service Section.
Protect the University’s network, systems, and data. Coordinate with designated technical and security staff to ensure the confidentiality, integrity, and availability of University systems and ensure that appropriate and timely action is taken. Determine if an on-site technical security evaluation is necessary and if any mitigation steps will be required. Coordinate with the unit technical/security staff to assure that appropriate diagnostic, protective, remedial, and other actions are taken as necessary to protect University resources. Coordinate with the appropriate University offices (administrative compliance, the General Counsel, human resources, and graduate school) as well as external Internet Service Providers (ISPs) and law enforcement as necessary.

17.4.7 The Chief Information Officer (CIO)
The CIO has the following responsibilities regarding the University Information and Cyber Security Program:

- Designate a Cyber Security Officer (CSO);
- Develop and maintain a University information and cyber security program;
- Develop and maintain information security policies, procedures, and control techniques to address all applicable requirements;
- Ensure compliance with applicable information and cyber security requirements; and
- Report annually, in coordination with the other senior Level Executives, to the University President on the effectiveness of the University information and cyber security program, including progress of remedial actions
- Designate individuals who have the responsibility and authority for IT resources.
- Establish and disseminate enforceable rules regarding access to and acceptable use of IT resources.
- Establish reasonable security policies and measures to protect data and systems.
- Monitor and manage system resource usage.
- Investigate problems and alleged violations of the University
IT policies.

- Refer violations to the Office of the President.

17.4.8 The Cyber Security Officer (CSO)

- Head an office with the mission and resources to assist in ensuring the University's compliance with information security requirements;
- Periodically assess risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the University;
- Develop and maintain risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each University information system to ensure compliance with applicable requirements;
- Facilitate development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- Ensure that University personnel, including contractors, receive appropriate information security awareness training;
- Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities;
- Periodically test and evaluate the effectiveness of information security policies, procedures, and practices;
- Establish and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the University;
- Develop and implement procedures for detecting, reporting, and responding to security incidents;
- Ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of the University; and
- Support the University's CIO in annual reporting to the University President on the effectiveness of the University information security program, including progress of remedial actions.

17.4.9 System/Network Administrator

- Take reasonable action to ensure the authorized use and security of data, networks, and the communications transiting the system or
network.
- Participate and advise as requested in developing conditions of use or authorized use procedures.
- Respond to questions from users relating to appropriate use of system/network resources.
- Cooperate with appropriate University departments and law enforcement officials in investigating alleged violations of policy or law.

17.4.10 **Data Custodians**
- Grant authorized users appropriate access to the data and applications for which they are stewards, working with University data security and network personnel to limit access to authorized users with a legitimate role-based need.
- Review access rights of authorized users on a regular basis.
- Respond to questions from users relating to appropriate use of system/network resources.
- Implement and oversee processes to retain or purge information according to University records retention schedules.
- Determine the criticality and sensitivity of the data and/or applications for which they are stewards; determine which University data is public and private based on University definitions, in consultation with the University's Office of Document & Records Management [link: 12].
- Ensure that appropriate security measures and standards are implemented and enforced for the data under their control – especially protected information - in a method consistent with Japanese law, University policies and sound business practices. The security measures implemented must be based on the criticality, sensitivity, and public or private nature of the data, and may include methodologies, change management, and operational recovery plans.
- Investigate problems and alleged violations of University IT policies.
- Refer violations to the Office of the President.

17.4.11 **University Academic Units and Administrative Departments**
- Create, disseminate and enforce IT use requirements that are consistent with University-wide policies set out in this Chapter for the University facilities and/or resources under their control.
- Audit the use of University resources under their control, and employ
increased monitoring if there are reasonable grounds to suspect violations of the requirements of this Chapter.

- Investigate problems and alleged violations of University IT policies.
- Refer violations to the Office of the President

17.5 Procedures

17.5.1 How to Request Access to IT Resources

17.5.1.1 Read the OIST Graduate University IT Resources Use Agreement [link: 17.6.1];

17.5.1.2 Understand the OIST Graduate University IT Resources Use Agreement [link: 17.6.1];

17.5.1.3 Sign (electronically) the OIST Graduate University IT Resources Use Agreement [link: 17.6.1] and

17.5.1.4 Submit (electronically) the OIST Graduate University IT Resources Use Agreement [link: 17.6.1]

17.5.2 Hosting Equipment in University IT Facilities

OIST IT offers hosting services for researcher purchased equipment within OIST IT facilities. This standard is in place to ensure that all equipment purchased and hosted in OIST IT facilities is suitable to facilities available, and that the hardware hosted in IT facilities is standardized where ever possible to minimize complexity and management costs. This standard also aims to ensure that equipment is of sufficient quality and functionality to enable users to control equipment remotely, and not need to rely on IT for simple operations such as console access, reboot, re-installation etc. This makes for a far better experience for the user and far simpler operation for IT, resulting in benefits to the University as a whole. Equipment to be hosted will require a consultation with OIST Information Services Section, and the approval of the CIO prior to purchase. This consultation ensures that sufficient network, power, space and cooling requirements are reserved for the equipment, and that it is suitable for hosting.

17.5.2.1 Please contact the Information Services Section to discuss any requirements you may have. A basic list of the requirements
on equipment intended to be hosted in OIST IT facilities is below. This list is by no means exhaustive, and requirements will vary depending on the specification of the equipment.

17.5.2.1.1 All equipment must include rails for mounting into 19” racks (of standard EIA-310-D).
- The equipment should be designed for a maximum rack depth of 30”
- All equipment must fit and secure correctly and safely into the rack

17.5.2.1.2 All hardware must come with in-built remote management capability allowing users to perform almost all actions themselves by remote. These capabilities must not involve additional licensing or software on the client system. The capabilities of the remote management controller should include;
- A dedicated (not shared), in-built, remote management interface with a standard 100Mbps or 1Gbps, UTP interface
- Full remote keyboard, screen and mouse control
- Full remote boot connectivity, i.e. the system can be remotely booted from a remote CD device
- Full remote power control (on, off, ACPI graceful shutdown)
- Full monitoring remote SNMP monitoring of:
  - Power (voltages etc.)
  - Temperatures
  - Disk health
  - Chassis health
  - Memory health
- Examples of remote management controllers include; Dell iDRAC Enterprise, IBM IMM with Virtual Media KEY, HP iLO.

17.5.2.1.3 Hardware should in general not be self built, and should be covered under and single vendor warranty.

17.5.2.1.4 Hardware warranty should be for at least 3, and preferably 4 years in duration, and cover all elements of the system.
17.5.2.1.5 Hardware should be redundant in any manner appropriate.
- RAID configurations are strongly recommended (hardware, not software raid)
- Redundant power supplies are strongly recommended for critical applications

17.5.2.1.6 Hardware should be of server quality, and not consist of desktop hardware which can be mounted into racks. Ideally the hardware should be manufactured by a reputable manufacturer and be specifically designed for rack mounting. Examples of server manufacturers include:
- Dell
- IBM
- HP

17.5.2.1.7 IT shall at all times have administrative/root level access to all systems housed in IT facilities, including any system and remote management interfaces. It is the responsibility of the user to ensure that this access remains valid, and that any changes that would affect this access are reported to IT. Exceptions and exemptions are to be determined by the CIO.

17.5.3 How to report IT abuse and security incidents

17.5.4 How to install non-university applications

17.5.5 How to purchase IT equipment

17.5.6 How to re-use or dispose of IT equipment

17.5.7 How to obtain a computer account for
- researchers
- staff
- students
- outside collaborators

17.5.8 How to gain access to privileged resources (e.g. HR, Finance, etc.)
17.5.9 How to obtain wireless access

17.5.10 Minimum cyber security rules for IT applications at the University

17.5.11 How to gain access to the University IT facilities

17.6 Forms

17.6.1 *OIST Graduate University IT Resources Use Agreement*

17.6.2 *Accessing OIST Graduate University IT Facilities*
1. OVERVIEW
Information resources of the University are subject to "appropriate use" requirements found in Japanese law and the University’s IT policies, rules, and procedures [link 17]. Access to and use of the University computer resources is conditional upon adherence to such law and policies.

2. PURPOSE
The purpose of this policy is to outline the acceptable use of the University information resources and to ensure that proper control is setup to maintain the confidentiality, integrity and availability of information processing and communication services on systems managed by the University. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, data leaks, and legal issues.

3. SCOPE
This policy applies to all students, employees, guests, contractors, consultants, temporaries and other workers at the University, including all personnel affiliated with third parties (“User”). This policy applies to all the University information resources, including but not limited to computers, systems and networks that are managed by the University and equipment not owned by the University but connected to the University network and/or using the University information resources.

4. POLICY
The University information resources are government-subsidized assets and may be used only for transactions related to the carrying out of the University mission and purpose. Unauthorized use is prohibited. Incidental personal use may be permitted if compliant with the Policy on Use of University Resources [link: 21] and reasonable in light of the person’s other obligations to the University.

Users have an affirmative duty to report immediately suspected misuse of the University information resources. Contact the Information Service Section help line [link: 17.7.2].

All the University policies apply to User’s conduct while using the University information resources especially, but not exclusively, policies on intellectual property, misuse of resources, harassment, and information and data.
The University computer accounts are normally intended for use only by the individual assigned to that account. Each account holder is responsible for the resources used by that account and for taking necessary precautions to prevent others from using the account. Shared accounts require adequate justification and explicit authorization from the CIO. Users shall not seek to gain or enable unauthorized access to information resources.

Passwords [link: 17.3.3] must be chosen with care and not divulged to anyone. Different classes of system (business systems, scientific computing systems) have different requirements on user passwords. Users are responsible for following the password policies for the systems on which they have accounts.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the University or the end user does not have an active license is strictly prohibited.

Before leaving a system unattended, it must be adequately protected, e.g. with a screen saver or logged off.

Users must safeguard legally protected information [link: 17.3.5] subject to privacy laws or confidentiality requirements.

Circumventing security controls is prohibited.

Under no circumstance is a User authorized to engage in any activity that is illegal under local, prefectural, national or international law while utilizing the University owned resources.

Use of the University's electronic communication facilities to send fraudulent, harassing, obscene (i.e. pornographic), threatening, racial, sexual or other unlawful messages is prohibited and illegal, as is use of the University’s information resources for lobbying of any kind.

The University has the right to audit and monitor networks and systems using the University information resources to ensure compliance with this OIST Graduate University IT Use Agreement and with other University policies and requirements related to IT access and use. IT equipment may
be confiscated, without notice, for forensic review with concurrence or direction from the General Counsel and/or the office of the Vice President for Administrative Compliance.

5. VIOLATION OF POLICY
Any University employee found to have willfully ignored or intentionally violated this Use Agreement or other University policies and rules related to IT access and use shall be subject to disciplinary action up to and including termination. A User violating this Use Agreement or other University policies and rules related to IT access and use may have his/her computer removed from the network and any University network or computer access disabled. Reinstatement will require the review and approval of the CIO, the President, and, in the case of student violators, the Dean of the Graduate School. Equipment may be confiscated for forensic review with concurrence or direction from the General Counsel and/or the Vice President for Administrative Compliance.

6. Exceptions to Policy
Any exception to this policy must be in writing and approved by the CSO with concurrence from the CIO.

7. Updating this policy
The CSO or his designee will update this policy as necessary to comply with new laws and regulations and will review it at least biennially.

Definition:
The term “users” applies to all University staff, contractors, assignees, visitors, and individuals that have custody of or access to the University information, systems, or network.
Appendix B: Using IT Resources

Use of IDs and Passwords
- Do not share your password(s).
- Your password should be made up of numbers and letters.
- Your password should not be a dictionary word.
- Change your password frequently.
- Understand that you are responsible for all activities on your username/account ID.
- Never give your password to any other person.
- Ensure that others cannot learn your password.
- If you have reason to believe that your username/account ID or password has been compromised, contact your System/Network Administrator immediately.

Use of Information/Data
- Access only accounts, files, and data that are your own, that are publicly available, or to which you have been given authorized access. Secure information that is in your possession.
- Maintain the confidentiality of information classified as private, confidential or data on decedents.
- Use University information for tasks related to job responsibilities and not for personal purposes.
- Never disclose information to which you have access, but for which you do not have ownership, authority, or permission to disclose. Keep your personal information/data current.
- Accurately update your own records through University self-service systems and other processes provided for you.

Use of Software and Hardware
- Use University e-mail, computers, and networks only for legal, authorized purposes. Unauthorized or illegal uses include but are not limited to:
  - Harassment;
  - Destruction of or damage to equipment, software, or data belonging to others;
  - Unauthorized copying of copyrighted materials; or
  - Conducting private business unrelated to University activities.
- Never engage in any activity that might be harmful to systems or to any information/data stored thereon, such as:
  - Creating or propagating viruses;
• Disrupting services or damaging files; or
• Making unauthorized or non-approved changes.
• When vacating computer workstations, sign-off or secure the system from unauthorized use.
• Use only legal versions of copyrighted software on University-owned or vendor computer or network resources, in compliance with vendor license requirements.
• Be aware of any conditions attached to or affecting the provision of University technology services:
  • Consult with the system administrator for any questions about system workload or performance.
  • Refrain from monopolizing systems, overloading systems or networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

For situations not covered here, contact your system/network administrator or departmental computer contact or send email to security@oist.jp.

*END OF FORM*
Accessing OIST Graduate University IT Facilities

Access to the University IT Facilities is ordinarily limited to persons carrying out preplanned or remedial activity, such as implementation, maintenance or incident-related work. Access for other purposes, such as site visits, must be prearranged through the Office of the CIO.

Those who will be physically located inside the University IT Facilities outside of normal business hours (09:00 – 17:30), must inform security: 098-966-8861 (Internal: 18861)

All those granted physical access to the University’s IT facilities must comply with the following requirements:

**Safety**
1. Comply with the University’s Safety & Health Management procedures:
   [link:]
2. Note location of emergency exits, fire extinguishers; and first aid kits.
3. Read emergency signage and maps.
4. If an emergency arises, follow instructions of the University staff in the area.
5. Safety incidents must be reported: 098-966-8989 (Internal: 18989)

**Rules of Conduct**
1. No misuse or abuse of any equipment within the facility.
2. Cleanliness and general housekeeping is to be observed:
   - Equipment must be unpacked and tested in the server room office before transport into the server room
   - All areas are to be kept in a safe and clean condition at all times
   - Any boxes, packaging or waste are to be cleaned up or removed after work is completed
3. Contact with equipment or systems outside/beyond the scope of approved works is not permitted.
   - Lifting of floor tiles without prior authorization from the University IT staff is prohibited
   - Undertaking cabling or electrical works without prior approval from the University IT is prohibited
4. Harassment or disturbance of others working on-site is not permitted.
5. Unauthorized photography or recordings are not permitted.
6. Food and Drink are not permitted.
7. Any activity violating the Universities policies or rules, or violating civil or criminal law, will be reported to the appropriate authority.

*End Of Form*
17.7 Contacts

17.7.1 Policy Owner
Chief Information Officer (CIO)

17.7.2 Other Contacts
Cyber security incidents must be reported to “security@oist.jp”
General IT questions, concerns, etc. must be addressed to “it-help@oist.jp”

17.8 Definitions

17.8.1 Acceptable Use
This term consists of these related concepts:
Information/data and systems may only be used by authorized individuals to accomplish tasks related to their jobs. Use of the information and systems for personal gain, personal business, to commit fraud or any other illegal activity is prohibited.
Information not classified as Public must be protected, and must not be disclosed without authorization. Unauthorized access, manipulation, disclosure, or secondary release of such information constitutes a security breach, and may be grounds for disciplinary action up to and including termination of employment.

17.8.2 Authorized User
Individual or entity permitted to make use of the University computer or network resources. Authorized users include students, staff, faculty, alumni, sponsored affiliates, and other individuals who have an association with the University that grants them access to the University IT resources. Some users may be granted additional authorization to access institutional data as authorized by the data owner or custodian.

17.8.3 Cyber Security
The protection of data and systems in networks that are connected to the Internet.

17.8.4 Data Custodian
Data custodians are representatives of the University who are assigned responsibility to serve as a steward of the University data in a particular area. Data custodians are responsible for developing procedures for creating, maintaining, and using the University data, based on the University policy and applicable local and national laws.
### 17.8.5 Default Custodians

Absent explicit arrangements to the contrary, the custodian of an asset is taken to be:

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Default Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core System - Finance</td>
<td>Vice President for Financial Management</td>
</tr>
<tr>
<td>Core system - Human Resources</td>
<td>Vice President for Gender Equality and Human Resources</td>
</tr>
<tr>
<td>Sakai system - Student Administration</td>
<td>System’s Administrator</td>
</tr>
<tr>
<td>Major University system - other</td>
<td>Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>University Network</td>
<td>Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>IP telephony system</td>
<td>Chief Information Officer (CIO)</td>
</tr>
<tr>
<td>Library systems</td>
<td>University Librarian</td>
</tr>
<tr>
<td>Computer laboratory</td>
<td>Head of organizational unit that provides the laboratory</td>
</tr>
<tr>
<td>University end-user computer allocated to a staff member</td>
<td>The end-user</td>
</tr>
<tr>
<td>Data residing only on an end-user computer</td>
<td>The end-user</td>
</tr>
<tr>
<td>USB storage devices and the like</td>
<td>The end-user who owns the device or to whom the device has been allocated</td>
</tr>
<tr>
<td>Servers (file, print, web)</td>
<td>Head of organizational unit that provides the server</td>
</tr>
<tr>
<td>University-owned IP-telephones allocated to particular staff or students</td>
<td>The end-user</td>
</tr>
<tr>
<td>Other University-owned IP-telephones (e.g. in meeting rooms and at service points)</td>
<td>Head of organizational unit that provides the room, service point or similar resource.</td>
</tr>
<tr>
<td>University owned mobile telephones within the scope of this policy</td>
<td>The end-user</td>
</tr>
<tr>
<td>Assets within the scope of this policy that are personally owned by staff, students or other individuals</td>
<td>The end-user</td>
</tr>
<tr>
<td>Assets within the scope of this policy</td>
<td>The affiliate or other external entity</td>
</tr>
</tbody>
</table>
17.8.6 **IT Resources**
Facilities, technologies, and information resources used for the University information processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, instructional materials. This definition is not all inclusive but rather reflects examples of the University equipment, supplies and services.

17.8.7 **Information Security**
The protection of data against unauthorized access. Programs and data can be secured by issuing passwords and digital certificates to authorized users. However, passwords only validate that a correct number has been entered, not that it is the actual person. Digital certificates and biometric techniques (fingerprints, eyes, voice, etc.) provide a more secure method (see authentication [link: ]). After a user has been authenticated, sensitive data can be encrypted to prevent eavesdropping.

17.8.8 **Security Incident**
An intentional or accidental occurrence affecting information or related technology in which there is a loss of data confidentiality or integrity, or a disruption and/or denial of availability.

17.8.9 **Security Measures**
Processes, software, and hardware used by system and network administrators to ensure the confidentiality, integrity, and availability of the IT resources and data owned the University and its authorized users. Security measures may include reviewing files for potential or actual policy violations and investigating security-related issues.

17.8.10 **Personal Shared Web Server Account**
An account and directory on a shared web server the maintenance and backups of which will be performed by IT; however, no support from the University is provided for the contents and use of the web space in the account.
17.8.11 **Dedicated Virtual Machine**
Virtual machine instances for research and software development projects. While the server hosting the VM will be maintained and backed up by IT, the contents and functionality of the system inside the VM is solely the responsibility of the user(s). No support will be supplied by the University staff for the system(s) inside the VM.

17.9 **Appendices**