Acceptable Use Policy (AUP) version 1.7

1. OVERVIEW

Access to and usage of Okinawa Institute of Science and Technology Graduate University Information Technology Resources (herein OIST IT Resources) is subject to Japanese law and the University's policies, rules, and procedures in Information Technology and Security (herein PRP17). Access to and use of OIST IT resources is conditional upon acceptance and adherence to these laws, PRP17, and other University policies and rules as agreed via acceptance of the Acceptable Use Policy stipulated herein.

2. Scope

This Acceptable Use Policy agreement applies to individuals or entities granted access to OIST information resources to a level beyond that available to the public; this includes but is not limited to students, employees, guests, contractors, consultants, temporaries and other workers at the University, including all personnel affiliated with third parties (herein Users).

This Acceptable Use Policy applies to all OIST IT 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 OIST IT Resources.

3. Rules

（1） All users are obligated to use OIST IT resources in an effective, efficient, prudent and responsible manner in support of the mission of the University and in line with relevant legal, contractual and professional obligations.
（2） Users shall adhere to the OIST respectful workplace policy, especially when communicating via email or other digital means
（3） OIST information assets (all information and data related to OIST business regardless of media format) are allocated a classification [LINK to OIST Information classification]. Users must treat OIST information assets in accordance with the restrictions associated with this classification.
（4） Users shall 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 [LINK to OIST Information classification→ access].
（5） Users shall comply with all provisions related to the management of user accounts, including:

- An account shall be used only by the individual to which is has been assigned.
- Each account holder is responsible for the resources used by that account and for taking necessary precautions including appropriate password management, to prevent others from using the account.
- Accounts are not to be shared, exceptions must be authorized by the CIO or CISO.
- Users shall not seek to gain or enable unauthorized access to information resources.

(6) Users shall comply with the following provisions related to OIST IT asset management.

- OIST IT devices except mobile devices shall be physically secured to prevent theft.
- Screen lock functions are to be configured to activate after a 5-minute idle period.
- Where users retain local administration rights to a device, they are responsible for;
  - Ensuring that security updates, and OIST prescribed anti-malware software are installed and up to date
  - Quarantining any malicious files detected by the anti-malware software
  - Ensuring that the real-time anti-malware inspection function is enabled
  - Periodically performing a full scan for malicious software

(7) Personal owned resources (Bring Your Own Devices, BYOD)

- Within administration BYOD is not permitted.

- Within research units, supervisors may choose to permit BYOD, and users may elect to use their own resources accordingly, though at no time should any user be compelled to do so. The supervisor and asset owner are accountable for any and all issues arising from the usage of such BYOD devices.
- All BYOD devices must be registered with OIST IT prior to accessing OIST IT resources.
- All BYOD devices are subject to PRP17 and must comply with all OIST requirements.

(8) Should users become aware of an information security incident they shall immediately contact the CISO and CIO via security-incident@oist.jp.

(9) General conduct

- Users must safeguard legally protected information subject to privacy laws and confidentiality requirements.
- Copyright law and licensing restrictions shall be respected at all times.
- 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.
- Use of OIST IT resources to send fraudulent, harassing, obscene (i.e. pornographic), threatening, racial, sexual or other unlawful messages is prohibited and illegal, as is use of OIST IT resources for lobbying of any kind.

4. VIOLATION OF POLICY

Any user found to have violated this Acceptable Use Policy, PRP17 or other University policies and rules related to OIST IT resource access and information security shall be subject to disciplinary action up to and including termination or termination of contract, and/or liable for compensation for all damages occurring to OIST. A User violating this Acceptable Use Policy, PRP17 or other University policies and rules related to OIST IT resource access and information security 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 CISO, the CIO, the President, and, in the case of student violators, the Dean of the Graduate School. Equipment may be sequestered for forensic review for a prescribed periods for litigation or other legal purposes under direction from the President or General Counsel, and upon consent of the CIO and the CISO.

Note to Students:

The computer supplied to you by the Graduate School remains the property of OIST until such time as it is legally disposed of by asset transfer. Accordingly, no unauthorized material (see above) may be stored on that machine at any time. By accepting the computer for your own use, you explicitly acknowledge that it may be subject to remote background analysis and monitoring at any time it is connected to the OIST network, and you may not circumvent attempts to do so in any way.

For situations not covered here, refer PRP17 or contact it-help@oist.jp.

I have read, accept, and agreed to abide by the conditions outlined above.

Company Name: _____

Name: _____

Signature: _____

Date: _____

The signature is valid for 12 months