Ibaraki University Information Security Policy Guide

Center for Information Technology,   January 2019

What is the Ibaraki University Information Security Policy (iISP)?

The proper use of information assets is essential if the University is to operate effectively as a research and education institution. The Ibaraki University Information Security Policy (iISP), which consists of an information security measures policy and action guidelines to be implemented at Ibaraki University, has been prepared for the purpose of ensuring safe and effective use of the University's information assets. The iISP covers, in detail, the basic concept of and basic policy on what information assets must be protected, what threats they must be protected from, and how they should be protected, as well as policies, systems, operation regulations, security measure standards, and other matters.

The Ibaraki University Information Security Policy is posted here. (Only a portion of the content is available for viewing from outside the University.)
https://www.ibaraki.ac.jp/isp/

iISP Structure

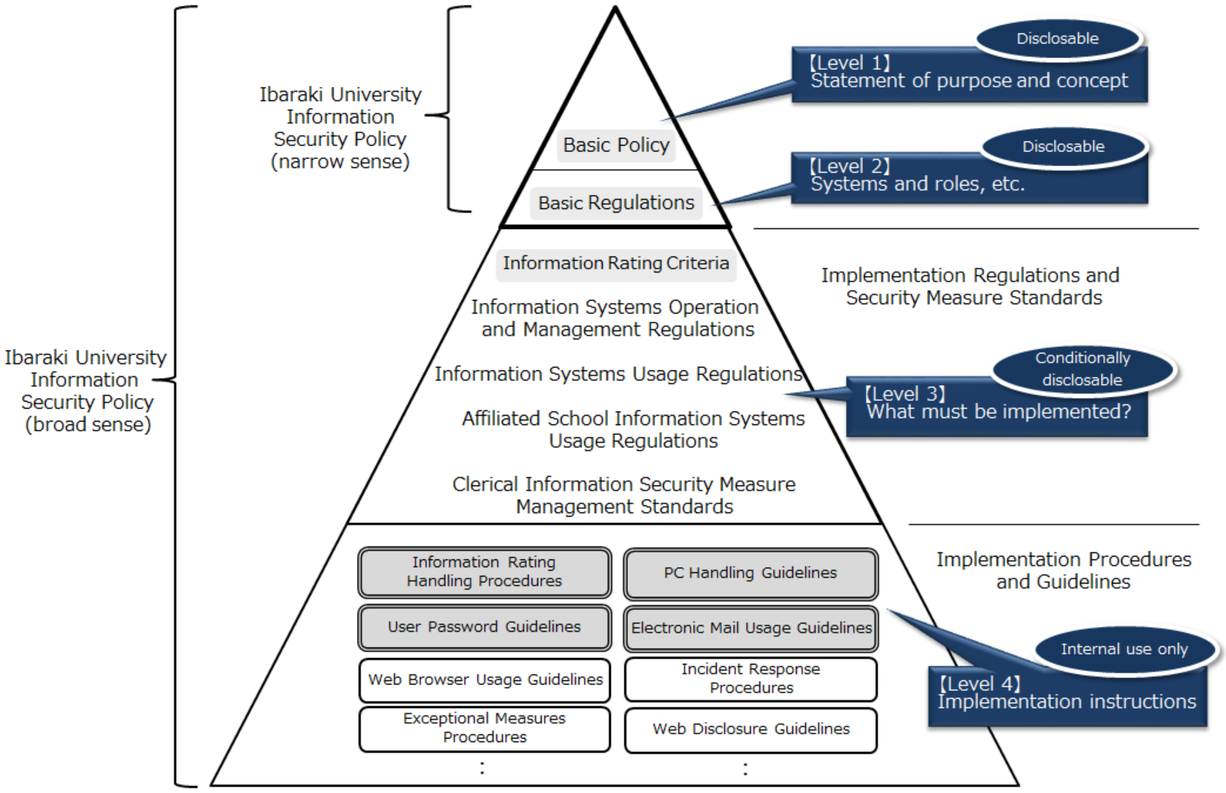
The iISP consists of the four levels shown below:

Level 1: The Basic Policy is a statement that indicates the purpose and concept of the iISP.

Level 2: The Basic Regulations stipulate systems and roles for implementing the iISP.

Level 3: The Implementation Regulations and Security Measure Standards stipulate what must be implemented.

Level 4: The Implementation Procedures and Guidelines are written instructions on how to implement the Level 3 Implementation Regulations and Security Measure Standards.


Ibaraki University Information Security Policy (narrow sense)
Ibaraki University Information Security Policy (broad sense)
Basic Policy
Basic Regulations
Disclosable
【Level 1】 Statement of purpose and concept
Disclosable
【Level 2】 Systems and roles, etc.
Information Rating Criteria
Information Systems Operation and Management Regulations
Information Systems Usage Regulations
Affiliated School Information Systems Usage Regulations
Clerical Information Security Measure Management Standards
Implementation Regulations and Security Measure Standards
Conditionally disclosable
【Level 3】 What must be implemented?
Information Rating Handling Procedures
PC Handling Guidelines
User Password Guidelines
Electronic Mail Usage Guidelines
Web Browser Usage Guidelines
Incident Response Procedures
Exceptional Measures Procedures
Web Disclosure Guidelines
:
:
Implementation Procedures and Guidelines
Internal use only
【Level 4】 Implementation instructions

Scope of Application of the iISP – What to Protect and Who Must Protect It

What? The iISP covers **all information assets that the University controls.**

The term “information assets” refers not only to information itself but also to the framework for managing information and information concerning the framework. Specifically, this includes internal network environments (wired LAN, wireless LAN), mail environments, PCs, software, various servers, various work data (including printed matter), and other information assets ranging from tangible information equipment to intangible information and software.

Who? The iISP covers **all persons who use the University’s information assets.**

Not only the University’s officers, faculty and staff, and students (including international students, Auditor, special Auditor, In-service Teachers, research students, and other equivalent non-degree students), but all persons who use information assets, such as dispatched workers, business operators who perform work for the University, and temporary ID users, are required to observe the iISP.

What to do when an incident occurs or is suspected

The term “incident” refers to an accident pertaining to information: a phenomenon or event that threatens information assets, such as information loss, alteration, leakage, or system failure due to a disaster. The iISP covers not only cases where an accident has actually occurred but also cases where an accident might occur. When an incident has occurred, the resulting damage is not always limited to individuals or contained within the University. Some incidents may have an enormous impact on society and jeopardize University management itself. When all users of the University’s information assets properly observe the iISP, it becomes possible to prevent incidents or minimize damage in the event an incident.

If you have discovered an incident or are concerned about a possible incident, contact CSIRT!

CSIRT Contact Information
Mail: csirt@ml.ibaraki.ac.jp
Telephone: 029-228-8750 (Mito) / 0294-38-5014 (Hitachi) / 029-888-8623 (Ami)

What is CSIRT?: CSIRT (Computer Security Incident Response Team) is a dedicated team for information security measures that performs a central response role when an incident occurs. The team consists mainly of Center for Information Technology staff members.

Required Precautions

1. Appropriately manage accounts

- Be sure to password-protect PCs, smartphones, and other devices that you use.
- Never give out a password to someone else. Never post a password where others can see it.
- Never let someone else use your account.
- Do not use the same password repeatedly. Attempted unauthorized access using passwords previously divulged or leaked on external websites is an everyday occurrence.

2. Protect PCs from virus infection

- Be sure to update Windows, MacOS, Linux, and any other operating systems used.
- Be sure to install antivirus software and update the virus definition files. Tens of thousands of viruses and other malware are newly created each day. Although no antivirus software can cope with every threat, it is far safer to use antivirus software than to take no precautions at all.

3. Take care not to leak information

- Beware of loss or theft of USB memory devices or PCs. Use encryption when storing information for University internal use only.
- **Never disseminate information restricted to within the University** using Twitter or other social networking services, or on personal blogs**. Additionally, never use such networks for University internal administrative communication.**

4. Do not use rogue software.

The term “rogue software” not only refers to malicious software created with the intention of causing harmful operation such as viruses but also includes software modified from commercial software and pirated software with copy protection removed. Not knowing software is illegal or rogue is no excuse. Beware of software of dubious origin or licensing circumstances.

5. Do not violate licenses

- Promptly uninstall software whose license is voided because of leaving your job, graduation, or other circumstances.
- Do not possess or use software or content that is not legitimately licensed.
- Do not continue to use software whose manufacturer support has expired.

6. Practice appropriate software management on University-owned PCs

- Faculty and staff are responsible for software management on university-owned PCs and other devices.
- Students must not install software on University-owned PCs or other devices without permission from a faculty member.

7. Use email with care

- Carefully confirm email addresses. (When a mail address has been automatically completed, confirm that it is not the address of someone else with the same name.)
- When simultaneously sending an email to multiple persons, there is a risk of leakage of information that should not be shared among all recipients. Be sure to use the BCC function and take other precautions. (For instance, an email notification of a medical checkup reexamination is medical information and it is necessary to ensure that it is not disclosed to others.)
- If you receive an email that elicits personal information, an email that prompts confirmation or updating of a bank account personal identification number (PIN), an email that demands money, an email that directs recipients to an illegal website, or the like, ignore it. If you have any concerns, contact CSIRT.

8. Acquire literacy as an information sender

- When you disseminate information using Twitter, Facebook, LINE, or any other social media, take responsibility for the information content because it may be viewed by the general public. Take particular care to ensure that retweets do not spread misinformation.
- Exercise caution in handling your own personal information. Did you yourself disseminate information on the Internet or has such information ever been leaked?
- Be aware that some website questionnaire pages are designed specifically for the purpose of collecting personal information and that some websites can collect operation history even before the “Send” button is pressed.