In Order to Keep a Secure Research Information Environment in JAIST

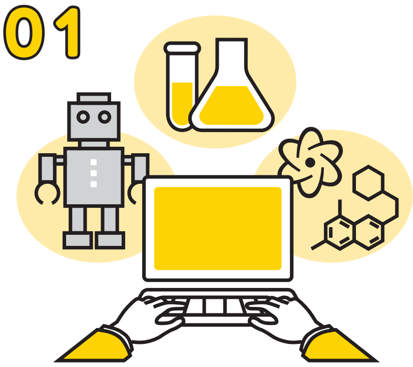
INFORMATION SECURITY PAMPHLET

Computers and the Internet have become indispensable for research and daily life activities. On the other hand, it involves various risks and misusage could threaten your research and data and might ruin your life.JAIST has established information security policies and social media guidelines to protect your research and data. As a JAIST member, you must surely comply.

Please carefully go through the checklist in the last page of this security pamphlet before using JAIST information environment. If you find anything unclear, please read the descriptions in the pamphlet and use the information environment in compliance with the rules.

Information Security Measures

01



Before Using : Understand JAIST ICT Environment is for Education / Research

It depends on the nature of each individual research to define what kind of usage is acceptable. In case of a student, it's up to the supervisor to decide if the purpose is acceptable or not. If you can not judge by yourself, please consult your supervisor.

02

Do Not Use a Weak Password; Do Not Tell Your Password to Others

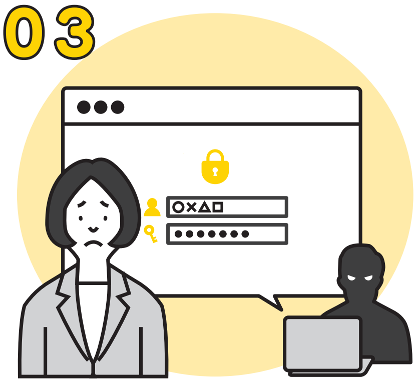
A strong password should be complicated enough for others not to guess (*). There have been cases of unauthorized access due to password violation when using the same passwords for other off-campus services. We recommend using password management software and not sharing passwords. Of course, you should not give your username or password to others. If you do, you will be responsible for anything that may happen.

JAIST staff will never ask you to disclose your password.

*We recommend that passwords are 10 or more characters with a combination of character types (uppercase, lowercase, codes, and numbers) and still easy for you to remember. Passwords can be easily guessed if based on personal names, birthdates, phone numbers, keyboard layouts, etc.

For more information, please refer to the "Supplementary Information and Links" listed at the end.

03



Do Not Make Unauthorized Access (Do Not Use Someone Else's Account)

Please note that criminal or civil offenses could include hacking and unauthorized access through security loop holes in addition to accessing services with somebody else's account or disguising identity or performing DoS attacks even if non-intentionally.

04

Regularly Update your OS and Applications to the Most Recent Versions

Computer viruses will take advantage of the vulnerability of popular software (Windows and macOS, Office, Java, etc.).

Regularly follow Windows and other Software Updates to always keep up to date. We recommend that you set your devices to automatically get the latest security patches.

Thus, please keep updating all the equipment connected to the network such as smartphones, wireless LAN routers, Internet Home Appliances, other IoT equipment and network devices.

05

Use JAIST-Specified Anti-virus Software and Always Use the Latest Virus Definition Files

PCs infected with malware may be remotely controlled and used for distributing spam or attacking elsewhere in addition to generate direct damage or destruction/leakage of data. Malware can spread not only by email transmission but also from webpages, flash drives, etc. Use antivirus software (*) in conformance with JAIST requirements and regularly update the virus definition files to prevent malware.

*Although different antivirus software exists, the performance of some of which is questionable. Therefore, JAIST has established specifications of usable antivirus software; for more information, please refer to the “Supplementary Information and Links” listed at the end.

06

Be Careful Not to Open Phishing Emails or Suspicious Webpages

Be careful of phishing emails pretending to be a bank, credit card company, cellphone company, or portal site in order to steal your personal information. If you receive any suspicious email, please do not contact the contact information in the email but contact directly the company.

Do not access any websites found on a social networking site or by search engine who market pirated software, copyright infringing animation/music/manga products, illegal drugs/weaponry/porn, or disclosing personal information. You could be punished for such illicit activities aside from being infected with malware.

Information Security Measures

07

Ensure Correct Management of Personal Information / Research Data and Take Information Leakage Precautions

Various education/research activities are underway on campus involving the handling of documents and data on personal information and research. Students as well as faculty and staff may handle personal information for research data and lectures on their own research.

Please properly handle the data and university documents according to JAIST Information Rating Guidelines. Moving research data outside the country may be restricted, especially data that can be diverted for other purposes, including weaponry and military involving national security. When sending emails, please be careful not to send to wrong addresses or mishandle them.

08

Do Not Copy Other Authors' Work Illegally or Make Them Available Online to Third Parties

That includes books, papers, reports, music images, software and applications. It is illegal to copy any work or make it available online without the consent of the author or beyond the extent permitted by law.

It is also illegal to knowingly download music or images that infringe copyright.

09

Put Information on the Internet Including SNS Responsibly as a JAIST Member

Statements and actions on the Internet can be seen by many; casual personal writings may lead to problems and cause situations where the credibility of JAIST or its members would be doubted. Be careful not to put inappropriate information, including information that should be kept secret or against public consensus and good manners. Please understand JAIST social media guidelines and the basic principles for posting information on social networks.

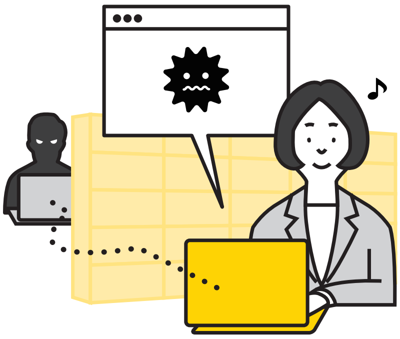
10

Do Not Allow Outsiders to Access JAIST Network

Except for authorized guests it’s unacceptable to provide outsiders with connectivity to JAIST LAN, (wireless/wired) which will lead to accessing information and services provided exclusively for the campus, which endangers the entire campus security.

In addition, using a VPN or data-anonymizing application on campus for such purposes as avoiding censorship will lead to providing others with Internet connectivity and allowing users all over the world to access campus-exclusive information, which is extremely dangerous. Do not use such applications on campus.

11



Do Not Use Applications Violating Laws or Threatening Security

Be careful of applications seemingly convenient but with unfamiliar mechanism; such as, file sharing applications (especially, P2P type).

Such applications can automatically transmit and forward files that might be an illegal act.

Before using any applications likely to violate laws or threaten security, please fully investigate how it works or how it is reviewed and consult the supervisors or RCACI.

*Examples of applications very likely to violate the laws or threaten the security

- ● Data anonymizing like VPN for bypassing limitations
  VPNgate, Tor, Hotspot Shield, SpotFlux, Hola Unblocker, Mobility XE, Freenet, Hamachi, etc.
- ● File sharing applications capable of automatic public transmission
  Xunlei, LimeWire, Cabos, Winny, WinMX, Share, eMule Parfet Dark, etc.

12

Keep the Contacts for Consultation /Reporting about Information Security Problems

Perpetrators’ technology is evolving each year. No matter how careful you are, you can become a victim of phishing or infected with malware. In this case it’s crucial to report and consult promptly.

Please contact JAIST CSIRT (*) immediately if any of your devices is infected with malware, or finding any of the following cases; vulnerability or failure in the security of JAIST information system - copyright infringement activity - leakage of confidential information / personal information - JAIST confidential information / JAIST member’s personal information disclosed outside JAIST.

*See the next page for contact information for JAIST CSIRT

CHECK!

01 □ Before Using : Understand JAIST ICT Environment is for Education/ Research

02 □ Do Not Use a weak Passwords; Do Not Tell Your Password to Others

03 □ Do Not Make Unauthorized Access (Do Not Use Someone Else’s Account)

04 □ Regularly Update your OS and Apps to the Most Recent Versions

05 □ Use JAIST-Specified Anti-virus Software

06 □ Be Careful Not to Open Phishing Emails or Suspicious Webpages

07 □ Ensure Correct Management of Personal Information/ Research Data and Take Information Leakage Precautions

08 □ Do Not Copy Other Authors’ Work Illegally or Make Them Available Online to Third Parties

09 □ Put Information on the Internet Including SNS Responsibly as a JAIST Member

10 □ Do Not Allow Outsiders to Access JAIST Network

11 □ Do Not Use Applications Violating Laws or Threatening Security

12 □ Keep the Contacts for Consultation /Reporting about Information Security Problems

Some cases can be exempted for justifiable reasons including research purposes.
If needed, please inquire to confirm in advance by asking the contacts listed below.

Contact for Consultation/Reporting about Information Security Problems

JAIST CSIRT

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

✉ E-mail
sec-incident@ml.jaist.ac.jp

Report URL
https://www.jaist.ac.jp/csirt/

Supplementary Information/ Links for the Pamphlet
https://www.jaist.ac.jp/iscenter/security/

☎ **0761-51-1300**
(RCACI/daytime and weekdays)

☎ **0761-51-1000**
(Disaster Prevention Center/nighttime and holidays)

Produced by : JAIST Research Center for Advanced Computing Infrastructure (2021.09)