The increased use of the Internet has brought with it a certain amount of convenience, and support has been provided for online classes or remote work. However, there are also problems caused by users not abiding by Internet etiquette, and network crime is on the rise. Especially, the time and expenses spent for repairing damage caused by virus infection - due to lack of security measures, being a victim/cause of secondary damage of unauthorized access or information leaks due to carelessness - cannot be ignored.

In order to protect the important information capital owned by Kyushu University at anytime and anywhere, it is important for us to implement information security measures and an information security policy, to prevent the utilization of information for false purposes, unauthorized access to our networks, information leaks, and other such incidents. Members of staff must have a strong awareness of information security measures, and strive to prevent incidents, while at the same time, implementing swift countermeasures if an incident does occur, and strive to prevent secondary damage from occurring. The University communications route for notifying any such incident, as well as the measures required for investigating, responding and reporting any such incident, are defined by the Information Infrastructure Initiative.

If you become a victim and cause secondary damage at the same time, you will experience emotional distress from spending a large amount of precious time repairing the damage. To prevent causing such incidents through improper use of the computer network, please be careful at home as well as at the University.

**〇Security policy**

In order to ensure that Kyushu University faculty members, students and other users can utilize the networks, calculation functions and other information infrastructure with peace of mind, we have defined a basic information security policy that must be strictly adhered to by those providing the relevant infrastructure, and by all those using it. When in doubt about the use of information assets, please refer to the security policy and stick to the operational rules. When you use devices belonging to the University at home, please make sure to follow the rules of the University as well as your department. Especially, follow the rules set by the University according to the confidentiality of the information.

**★For more details**

・Rules on information ethics of Kyushu University

https://www1.g-reiki.net/kyushu-u/reiki_honbun/u437RG00000140.html

・Kyushu University Information Security Policy

https://www.sec.kyushu-u.ac.jp/sec/policy/policy.html

・Kyushu University Information Security Measures and Regulations

https://www1.g-reiki.net/kyushu-u/reiki_honbun/u437RG00000131.html

**〇Measures to deal with copyright infringement, information incidents, and compliance with laws**

When using the computer network, make sure you are in compliance with laws. Never commit illegal acts such as the use of a non-genuine copy of Windows which is a copyright infringement and a license violation, or any other unauthorized use of commercial software. Making profits from the mining of cryptocurrency on campus is forbidden since it is considered an improper use of information devices and electricity.

Kyushu University restricts the use of all software that could lead to illegal acts such as the infringement of copyright, or result in the leaking of personal or other information. Please do not use this type of software at the University as well as at home. Please uninstall such software if it was installed before entering the school. There is a restriction on accessing websites which could lead to illegal acts such as the infringement of copyright on campus. In case it is necessary to access it, however, for education and research reasons, the restriction can be lifted through request. All access from outside the campus to inside the campus is restricted in general to prevent various cyber-attacks via remote internet access. In case it is necessary to access it, however, for education and research reasons, the restriction can be lifted through request.

**〇Learning and Self-check regarding information security measures**

To improve security measures university-wide, e-learning as well as self-checks regarding information security, have been conducted every year for all the university faculty and administrative staff.

- ＊Learning regarding information security measures
  All the faculty and administrative staff must take e-learning to improve knowledge and awareness regarding information security measures.
- ＊Self-check regarding information security measures
  All the faculty and administrative staff conduct self-checks with an online questionnaire regarding the basic information security measures of information security policy.

**〇Information security measures**

Listing examples of security threats in view of recent security incidents to take information security measures.

- ・Be aware of suspicious e-mails
  Many suspicious e-mails have been received targeting Kyushu University faculty and administrative staff. Many of the contents do not appear to have bad intentions. It is important to be security-conscious and suspicious regarding e-mails you receive. Comprehensive judgement is needed to discern suspicious e-mails and careful examination of the contents of the e-mail from various aspects is necessary. Furthermore, when information to join a web conference is received via e-mail, please carefully make sure the URL is correct.
  If you receive a suspicious email, please report it to the Kyushu University CSIRT. Sending suspicious e-mails you received to your department for the purpose of calling attention to it is dangerous and could lead to spreading the damage. In fact, an incident was reported in which a forwarded e-mail within campus contained malware. If you receive a suspicious e-mail, make sure to contact the Kyudai CSIRT first.
- ・Managing passwords
  When setting up a password, please follow the Kyushu University password policy. (*Please refer to “ Single Sign-On Web Portal / Kyushu University ” for more details.) If passwords for SSO-KID or other systems do not follow the Kyushu University password policy, change the password immediately. Moreover, reusing the same password could make you the target for password list type attacks, so do not reuse the same passwords and manage them properly. Do not tell others your passwords or ID (such as SSO-KID) unnecessarily.
- ・Virus Countermeasures
  Install an anti-virus software such as Windows Defender to protect your computer from computer viruses. Make sure the computer you are using at the University now has active anti-virus software. Update the virus definition file so that the anti-virus software is the newest version.
- ・Preventing information leakage
  The most common incidents when using University devices outside the workplace is loss and theft. When it is necessary to take out your work PC or USB with personal or confidential information in it, please manage the information assets properly while following Kyushu University Regulations for the Management of personal information as well as the rules of your department.

**○Other things you need to be careful of**

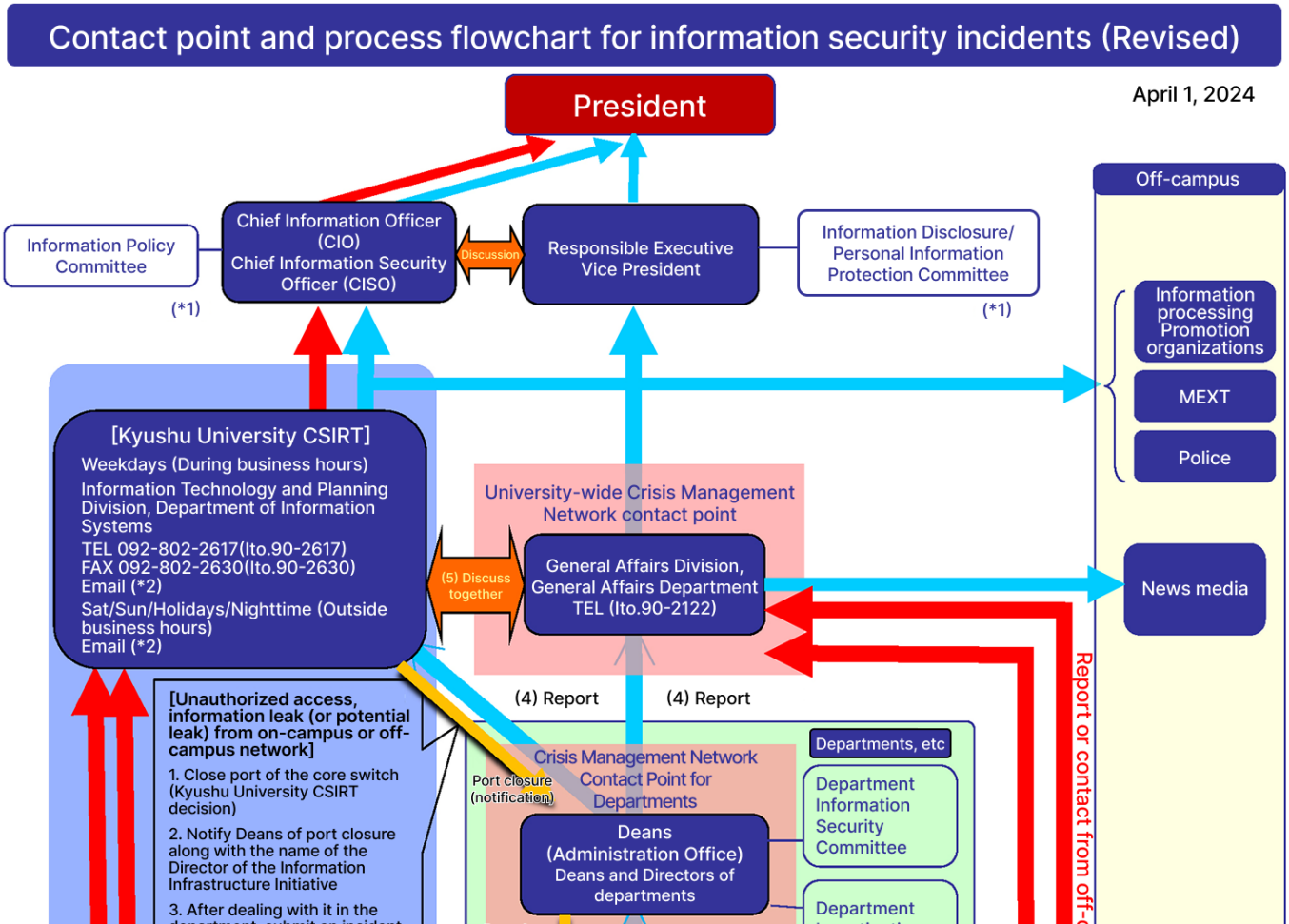
- ＊Do not lend your ID to others
  Do not allow your friends or others off campus to access the on-campus network or computer/smartphone authentication with your university-wide ID (SSO-KID, Student ID). If a friend who uses your computer causes an information incident, you will also be held accountable for that.
- ＊Avoid inappropriate use of social media or bulletin boards
  Please avoid inappropriate or extreme posts on social media such as X (formerly: Twitter), Facebook, LINE or online bulletin boards. Because of its anonymity, some have posted extreme comments on social media and this has resulted in inquiries to the University, or in some cases, one ’ s identity being revealed to the public. Even if posted anonymously on the internet, after some research, the source can be identified. The Social Media Usage Guidelines for Kyushu University Members have been established for fiscal year 2025.
- ＊Understand new threats
  Every year attacks with new methods are confirmed, such as Tech Support Scams and bank transfer fraud using a short message service.

Check the newest information on threats provided by the IPA regularly. By understanding the information on threats, harm can be prevented.
IPA (Information-technology Promotion Agency): https://www.ipa.go.jp/security/security-alert/

**○Flow of response when an incident occurs**

If an information security incident occurs (either externally or internally inflicted), it is necessary to identify this as early as possible, and take measures to prevent the situation developing any further. In such a case, please promptly submit an initial report to Kyudai CSIRT in accordance with the flowchart below titled "Communication and Response Flow in the Event of an Information Security Incident." Please communicate the details of the incident using the document formatted for an Information Security Incident Report.

# Contact point and process flowchart for information security incidents (Revised)



# Contact point and process flowchart for information security incidents (Revised)

December 1, 2021

**Weekdays** (During business hours)

Information Technology and Planning Division
Department of Information Systems

TEL : 092-802-2617 (Ito 90-2617)
FAX : 092-802-2630 (Ito90-2630)
E-mail : sec-inicident@iii.kyushu-u.ac.jp

**Sat/Sun/Holidays/Nighttime** (Outside business hours)

E-mail : sec-inicident@iii.kyushu-u.ac.jp

**Police**
Report lost or stolen property

Report or contact from off-campus

**Department**
Superior
Senior Professor, Chairman
Director, Head of offices

(2) Contact and Report

(1) Emergency Contact

Off-campus witness

**Witness**

(1) Emergency contact

(2) Contact and Report
In case of lost or stolen PC

**Incidents**
Operational error such as accidental sending
Lost or stolen PC
Virus infection
Unauthorized access
Leak from on-campus/off-campus network
Cyber fraud
etc.

※ Send emails, make calls and report to departments following this chart.

※ Do not deal with reports from anonymous individuals.
(Reference) The website contains reports, etc. https://www.sec.kyushu-u.ac.jp/sec/sec-incident.html
(Supplemental) This is a University-wide flow chart.
If there is another flow chart based on this chart but unique to a department, please follow it.

## ★ Want to know more

・Website of the Information Infrastructure Initiative https://iii.kyushu-u.ac.jp/en/ ・Kyudai CSIRT Website https://www.sec.kyushu-u.ac.jp/kyudai-csirt-en/

## ◆ Contact

・Kyudai Computer Security Incident Response Team Matters concerning security incidents in general E-mail: sec-incident★iii.kyushu-u.ac.jp Suspicious e-mails E-mail: sec-info★iii.kyushu-u.ac.jp General Affairs and Public Relations Section, Information Technology and Planning Division, Information System Department Tel: 092-802-2617 ext.:90-2617 Section for Information Security, Information Technology Infrastructure Division, Information System Department Tel: 092-802-2685 ext.:90-2685