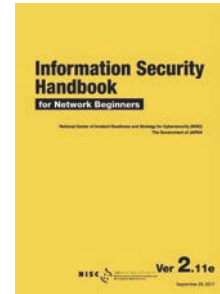# Information Security Checklist

This checklist can help you understand the basics of information security. Before using your devices on campus network, please read "Information Security Handbook" and check the following items. After understanding them, please check off all boxes and submit it to E2-5 Information Security Measures Group as in-house mail or send it to "contact@cert.titech.ac.jp" as an e-mail attachment.

Information Security Handbook
for Network Beginners

Ver **2**.11e

🔑 Password

☑ Do not reuse the same password on multiple sites.

You must never reuse the password of Tokyo Tech account as SNS websites such as Twitter or Facebook.

🔑 Password

☑ Use a long password as much as possible.

It must be at least 10 characters long including upper and lower letters, figures and symbols.

🔑 Password

☑ Do not store passwords near your PC.

Do not write passwords down near your PC or desk in plain sight.

📄 Software

☑ Install anti-virus software on your PC.

Symantec Endpoint Protection is available free of charge to all Tokyo Tech students, faculty, and staff.

📄 Software

☑ Keep your software and OS updated and patched.

It is prohibited to use unsupported software or OS (e.g. Windows XP, Vista) for business. Do not use old versions to prevent virus infections.

✉ E-mail

☑ Pay careful attention to the e-mails with attachments or links.

Never follow links or open attachments in suspicious or unsolicited messages unless you can verify the source.

🗄 Data Management

☑ Back up your important data.

Keep the backup data separated from the network.

🗄 Data Management

☑ Set passwords to files containing personally identifiable information.

Minimize the members who share the data containing personally identifiable information such as ID numbers, names, and passport numbers.

💼 Emergency

☑ Disconnect from the network if you suspect your PC is infected with a virus.

Unplug the LAN cable or disconnect wireless LAN while a power for the device is on.

💼 Emergency

☑ Contact the following addresses immediately if you suspect your PC is infected with a virus.

Do not try to solve the incident alone. Do not hesitate to contact CERT.
1. Your immediate supervisor
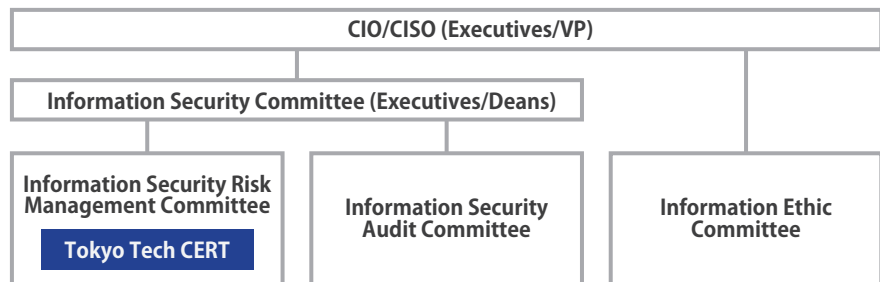2. Tokyo Tech CERT   Email: contact@cert.titech.ac.jp Ext: 3272

---

4 Basic Rules: everyone has to keep

1
Always keep OS and software
updated and patched

Automatic update is recommended.

2
Always keep anti-virus software
updated

Keep virus definition files up-to-date.

3
Never open suspicious e-mails

Beware of the sources and URLs/ attached file of e-mails.

4
Back up your data
regularly

Keep the backup data separated from the network to prevent it from encrypting by viruses (ransomware).

About Tokyo Tech CERT

"CERT" is an information security team at Tokyo Tech. We support students/faculty/staff to construct secure environments where they are able to concentrate on their own works. Our activities are "security incident response", "announcement of security issues" and "vulnerability scans". We focus on proactive efforts to reduce security incidents.

■ **Organization Chart**

CIO/CISO (Executives/VP)

Information Security Committee (Executives/Deans)

Information Security Risk Management Committee **Tokyo Tech CERT**	Information Security Audit Committee	Information Ethic Committee

May I help you ?

■ **WEB/Twitter**

WEB ： http://cert.titech.ac.jp   Twitter ： @T2CERT

If you think something is strange   ❶ **Detach devices from the network**   ❷ **Contact CERT**

Don't hesitate to contact us

[Contact]

MAIL：contact@cert.titech.ac.jp
Twitter：@T2CERT

東工大CERT
Tokyo Tech Computer Emergency Response Team
http://cert.titech.ac.jp

Information Security Checklist

Submission is required

Date： _____ Department/Institute： _____ Name： _____

> **This checklist can help you understand the basics of information security.**
> **If you have unfamiliar words, please ask the people nearby.**
>
> **Submit to Mail Box E2-5: Information Security Measures Group or**
> **Send to "contact@cert.titech.ac.jp" as an e-mail attachment**

🔑 Password

☐ **Do not reuse the same password on multiple sites.**

You must never reuse the password of Tokyo Tech account as SNS websites such as Twitter or Facebook.

🔑 Password

☐ **Use a long password as much as possible.**

It must be at least 10 characters long including upper and lower letters, figures and symbols.

🔑 Password

☐ **Do not store passwords near your PC.**

Do not write passwords down near your PC or desk in plain sight.

📄 Software

☐ **Install anti-virus software on your PC.**

Symantec Endpoint Protection is available free of charge to all Tokyo Tech students, faculty, and staff.

📄 Software

☐ **Keep your software and OS updated and patched.**

It is prohibited to use unsupported software or OS (e.g. Windows XP, Vista) for business. Do not use old versions to prevent virus infections.

✉ E-mail

☐ **Pay careful attention to the e-mails with attachments or links.**

Never follow links or open attachments in suspicious or unsolicited messages unless you can verify the source.

🗄 Data Management

☐ **Back up your important data.**

Keep the backup data separated from the network.

🗄 Data Management

☐ **Set passwords to files containing personally identifiable information.**

Minimize the members who share the data containing personally identifiable information such as ID numbers, names, and passport numbers.

🧰 Emergency

☐ **Disconnect from the network if you suspect your PC is infected with a virus.**

Unplug the LAN cable or disconnect wireless LAN while a power for the device is on.

🧰 Emergency

☐ **Contact the following addresses immediately if you suspect your PC is infected with a virus.**

Do not try to solve the incident alone. Do not hesitate to contact CERT.
1. Your immediate supervisor
2. Tokyo Tech CERT　Email: contact@cert.titech.ac.jp Ext: 3272