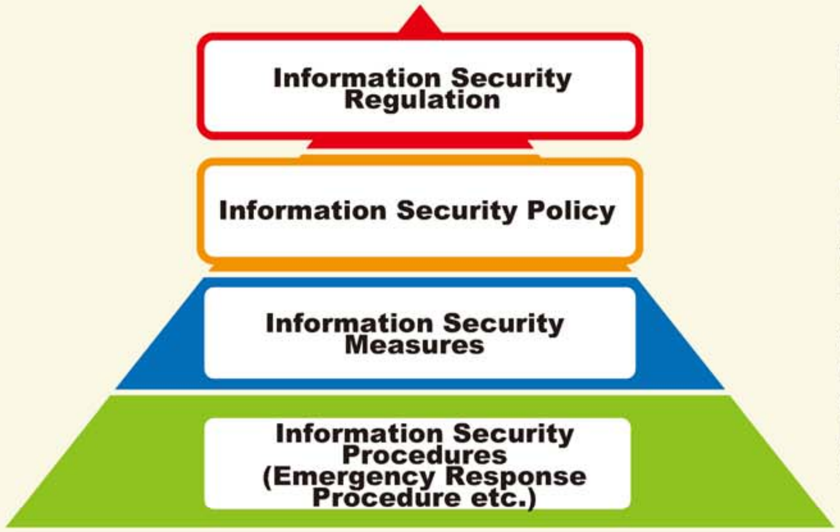
✓ Information Security Rules


Information Security Regulation

Information Security Policy

Information Security Measures

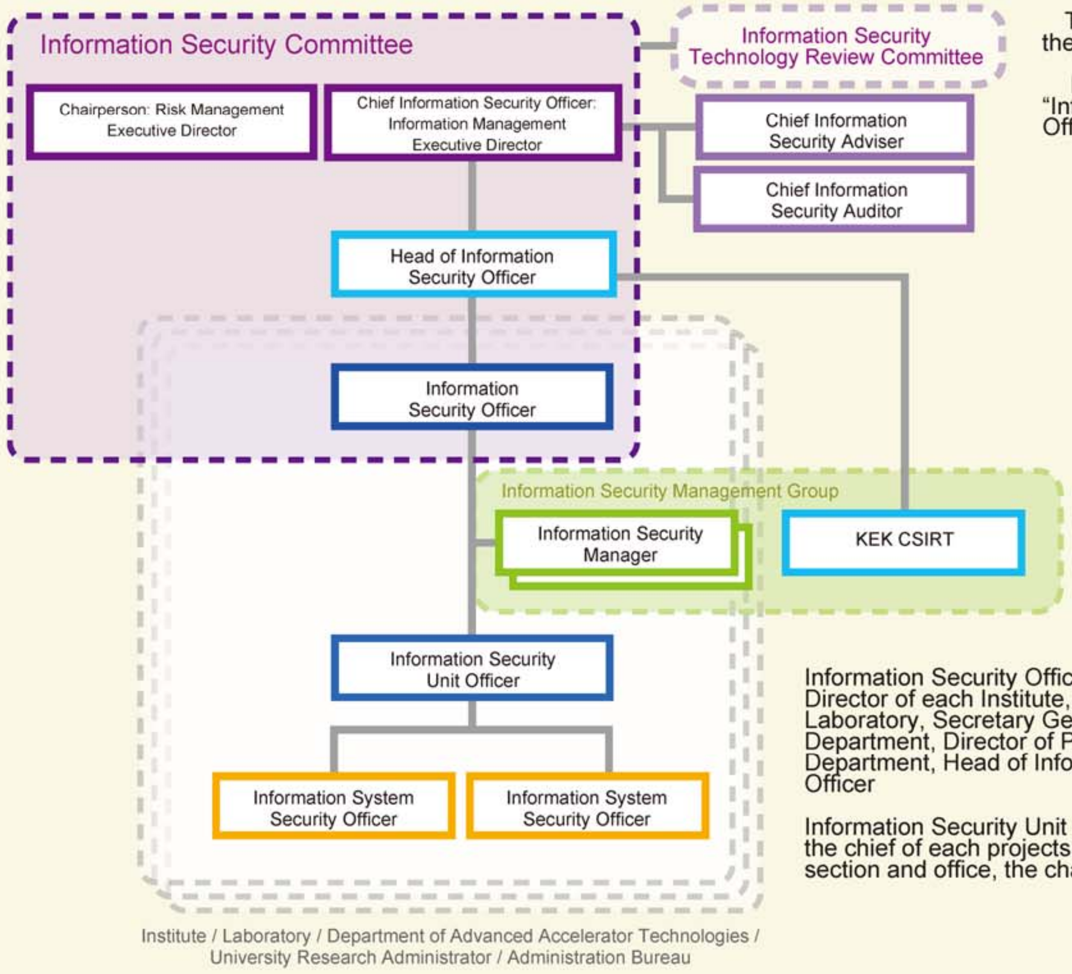
Information Security Procedures (Emergency Response Procedure etc.)

The rules of information security consist of four layers according to admission level, abstraction level of descriptions. Upper rule defines lower rule in detail.

"Information Security Regulation" and "Information Security Policy" notices the reason why we need information security, what and where to protect, who is a responsible person.
"Information Security Measures" define the things what to do according to upper rule and/or policy. Each measure has the definition of range and position.
Each procedure describes detail processes how to do.

Note: Information Security Rules are going to be corrected.

✓ Information Security Management Structure


Information Security Committee

Chairperson: Risk Management Executive Director

Chief Information Security Officer: Information Management Executive Director

Information Security Technology Review Committee

Chief Information Security Adviser

Chief Information Security Auditor

Head of Information Security Officer

Information Security Officer

Information Security Management Group

Information Security Manager

KEK CSIRT

Information Security Unit Officer

Information System Security Officer

Information System Security Officer

Institute / Laboratory / Department of Advanced Accelerator Technologies / University Research Administrator / Administration Bureau

To keep information security level, the management structure is defined.

PC user is usually assigned as "Information System Security Officer" .

Information Security Officer:
Director of each Institute, Director of each Laboratory, Secretary General, Director of the Department, Director of Public Relations Department, Head of Information Security Officer

Information Security Unit Officer:
the chief of each projects, the chief of each section and office, the chairperson or chief.

✓ Link About Rules and Structure

Refer links below.
https://stw.kek.jp/stpg/iso-e/ (English, browsing in KEK intranet only)
https://stw.kek.jp/stpg/iso/ (Japanese, browsing in KEK intranet only)

Computer Security 11 Best Practices -To Protect Your Computer-

2017.09.14 English Edition

email: kekinfosec@ml.post.kek.jp

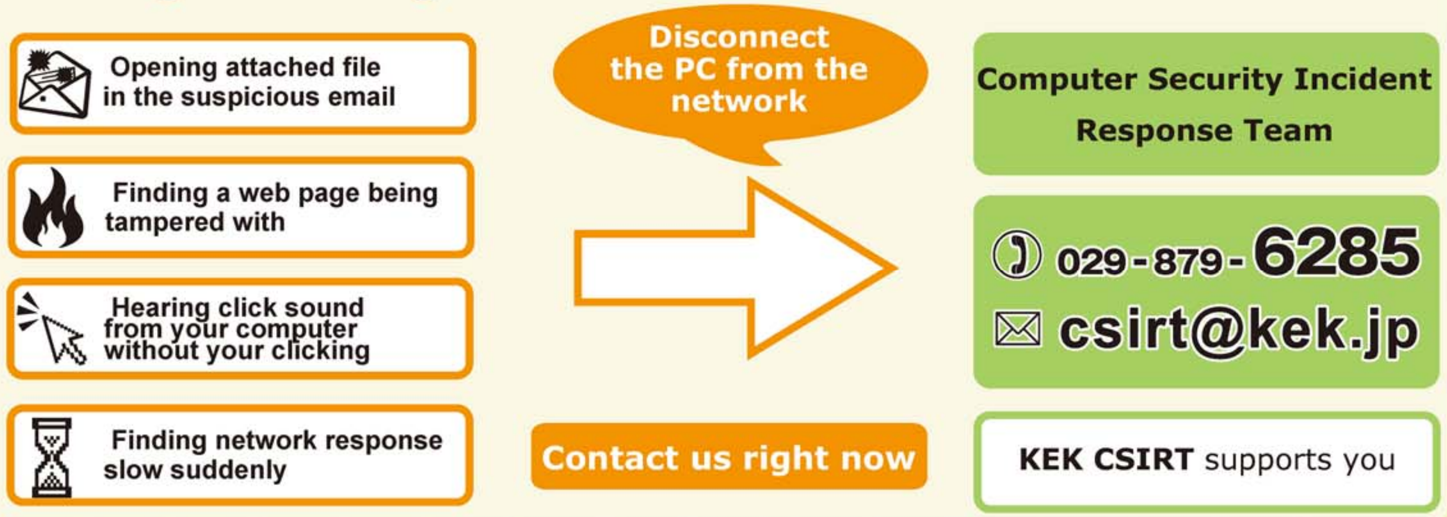
KEK

Computer Security

11 Best Practices

To Protect Your Computer

✓ Feeling something unusual


Opening attached file in the suspicious email

Finding a web page being tampered with

Hearing click sound from your computer without your clicking

Finding network response slow suddenly

Disconnect the PC from the network

Contact us right now

Computer Security Incident Response Team

☎ 029-879-6285
✉ csirt@kek.jp

KEK CSIRT supports you

KEK Computer Security 11 Best Practices

To Protect Your Computer

01 Update

Apply the latest security patches to OS and software on your devices.
- Also firmware/OS of network devices: printers, cameras, smartphones, routers etc.

Check update histories whether your PC is updated correctly.Reboot your PC when it is necessary.

02 Install Anti-virus Software and Schedule a regular full scan

Install anti-virus software.
- Activate anti-virus software properly.
- Update virus pattern database.
- Use the paid antivirus software.

A weekly scan is strongly recommended.

03 Password

Enforce strong passwords.
- A password needs enough length.
- Combine characters including upper and lower case, numbers, symbols.
- Do not use passwords that can be easily imagined.
- Each your account should have its own unique password.

****

Check login time and login histories to find login spoofing.

04 Web Browsing

Do not visit nor download and open any files from unofficial sites(e.g. suspicious website).
- Confirm whether the URL starts with "https" on the page which requests your secrets such as a password or a card number.
- Suspect that free service and freeware might have malicious activities.
- Suspect that popup page displays fake cautions.

You might have installed software unintentionally while web browsing. Check your installed program list regularly and delete the unintentionally installed software from your PC.

05 Add-ons, Plugins

The most of browsers have softwares called add-ons or plugins. The attackers often use the vulnerabilities of "Adobe Reader", "Adobe Flash Player", and "Java". Check your browser configurations regularly whether some add-ons or plugins are unintentionally installed.

Use the latest plugins. You can prevent the unintentional activity by setting plugin configuration to ask permission each time.

06 Email

Security incidents often occur by opening the attached file or by clicking a URL in the email body.
- Check the message whether "From" and "To" are known users or groups, that the body is related to your tasks.
- When you suspect the message, don't open the attached file and, don't access to the URL written in the mail body.

You should configure your mail software so as to use only plain text format.

07 Backup

The backups are good for rapid recovery and to minimize damages.

You need to manage backing up data and system periodically for backup.

You should backup your data and isolate it. Confirm the term of use and data treatment policy when you use the cloud service for backup except sensitve/important data.

08 USB Devices

Your PC might be infected when you connect a USB device to your PC.

Disable auto-play feature on your PC. Not only USB memories but also CD/DVD, smartphones, digital cameras etc. might have malwares.

Run anti-virus software before and after using USB memory. It is good to format USB memory after using it.

09 When you do not use your PC

Use screen lock when you leave from PC short time.
- Turn off your PC when you do not use PC for a long time to prevent malware infection.
- Submit a network disuse application as PC is no longer used.

Update your OS, anti-virus software and others when you reuse your PC after long shutdown.
A virus scanning is strongly recommended.

10 Handle Sensitive Data

Handle sensitive data, important and confidential data such as personal information and the secrets, on dedicated PC, not on the PC that you use for daily job.

When it is difficult, save sensitive data to the offline storage and connect it when needed. That makes your sensitive data safe.

11 Security Knowledge

Threats suddenly occur. The technique of social hacking is much improved recently.

The most important thing is to get the security knowledges.

You can get valuable information in the web site listed below.

Computer Securities of other Accelerator Laboratories

CERN Computer Security
https://security.web.cern.ch/security/home/en/index.shtml

Fermilab Computer Security
https://web.fnal.gov/organization/SecurityPublic/SitePages/Computer%20Security.aspx

IT Security at DESY
https://it.desy.de/services/it_security/index_eng.html

See Also

The public organizations - IPA, JPCERT/CC etc.- post the latest information about computer security. Moreover, there are some sites though it is nongovernment and post the security news. All links listed below are written in English.

IPA -IT Security-
http://www.ipa.go.jp/security/english/index.html

US-CERT
https://www.us-cert.gov/

CERT
https://www.cert.org/

JPCERT/CC Official blog
http://blog.jpcert.or.jp/

FIRST
https://www.first.org/

Security NEXT
http://www.security-next.com/

SecurityFocus
http://www.securityfocus.com/