Information Security Handbook

Department:

Name:

Point of contact for IT queries

Department:

Tel.: - -

Tel.: - -

Information Security Policy

AEON group principles are ‘pursuing peace’, ‘respecting humanity’ and ‘contributing to local communities’ while serving our customer. With these principles, we will recognize the importance of information security and protect important information from various threats to contribute to the society for safe and quality life.

We also believe that the information within AEON is a valuable asset for the development of business activities and the creation of value-added goods and services. To manage it in a safe and appropriate manner, we will build a solid relationship of trust with our customers, local communities, business partners and shareholders.

Information Security Policy is shown here to guide all employees of AEON group to be aware of and understand the importance of information security.

Established on September 1, 2019 Aeon Co., Ltd.

Initiatives for Information Security

We will execute the initiatives as stated below to ensure that all group companies are complied with the Information Security Policy.

1) Define roles and responsibilities to maintain and continuously improve information security
2) Establish and comply with security regulations to protect information security
3) Conduct risk assessment and implement security measures to protect information
4) Provide employees with security education to increase awareness of information security
5) Comply with laws and regulations as well as contracts with relevant stakeholders (e.g. customers, business partners and employees), having information properly managed
6) Establish clear reporting lines for fast and effective response for security incidents
7) Maintain information security level of subcontractors to a standard of being equal to or higher than that of AEON Group
8) Maintain business continuity by minimizing impact of natural disaster and cyber attacks
9) Conduct periodic and non-periodic review and internal security audit for continuous improvement of above activities
10) Penalties shall be applied for violation of this policy and information security regulations/ standards with accordance to the employment rules

Basic security rules

Prohibited Acts

Using devices other than corporate devices

Bring out corporate devices without permission

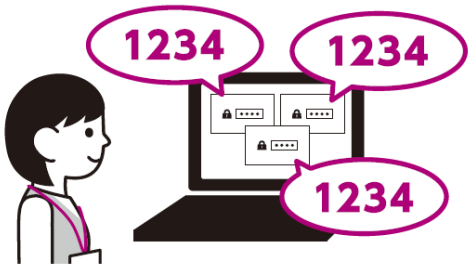
e.g. USB memory stick

Using external storage media without prior declaration

Personal web browsing on corporate devices

Using unauthorised software/service

Precautions

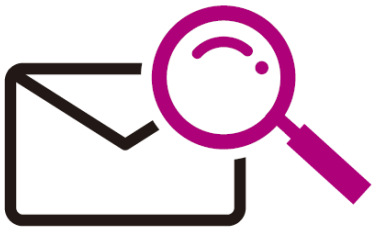


Reuse of same password

Carelessly clicking OK without checking

When using emails

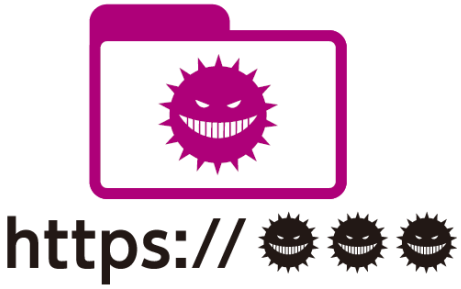
Precautions when received emails



Correct example:○○@aeonpeople.biz

Check if the email was sent from a right address.

Be careful when replying/forwarding.



Don't click suspicious files and links.

Precautions when sending emails

Be sure to check the contents and recipients.

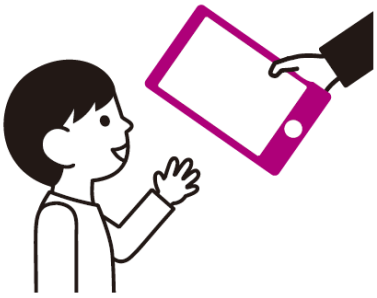
Protect confidential information with passwords.

When working remotely (off-site)

Prohibited Acts

Connecting to public Wi-Fi.

Carelessly making documents and/or recordings public.



Allowing your family to use corporate devices.

Precautions

Lock your screen when you leave your desk.

Always keep your devices with you when on the move.

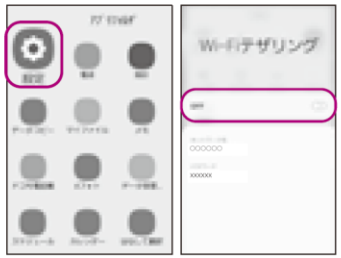
Important What to do if you get infected computer virus Steps to follow

Initial response

Any way, disconnect the network!

Detach LAN cable.

Disconnect Wi-Fi.



Turn off the tethering on smartphone.

As a last resort OFF! Power off the device.

Incident reporting

Promptly report to the company

Report Communicate Consult

Do not try to solve it yourself!
If you cannot get hold of anyone, don't panic; wait until you can establish contact.

Preservation of evidence

Preserve the evidence for investigation

Do not operate your PC.

Note: As a general rule, don't turn the power off.

Report immediately in the following cases

If any of the following happens, immediately report it to the emergency contact.

PC behaving abnormally

Repeate reboots itself.

Displayed unfamiliar notice.

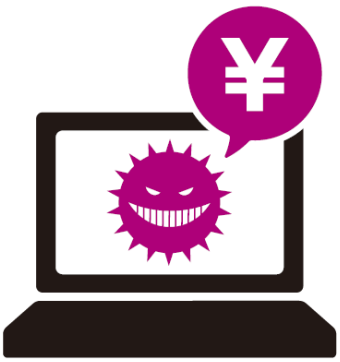
Unable to close the window.

Files are encrypted and cannot be opened.

Saved data is missing/ corrupted.

Contact by malicious third parties

Telephone number is displayed and demands contact.



Demands payment in return for repairing.

Demands payment by impersonating a business partner.

The flow of reporting

Detection of incident occurrence

Each business/company/shop

System maintenance provider

General Affairs Department of each company

IBS Divisional/ Departmental Manager

IT Department of each company (including financial services)

Incident reporting (understanding the situation)

AEON Co., Ltd. ICT Planning (Security Secretariat)/ General Affairs Department

Notice

30 minutes

Assessing the impact (understanding the impact)

Crisis management committee member

Depending on the situation, set up the incident response team

Store/Section Manager, Systems Chief

Notice

Notice

Each company's CEO/Head of Systems
Relevant departments of AEON Co., Ltd.

Chairman/CEO/Deputy CEO/Executive Director

30 minutes

Implement countermeasures