KOA Group Code of Conduct for Information Security

Date of Implementation: 1, July, 2014
Last Update: 12, March, 2018

1. Purpose of this Code of Conduct

This Information Security Code of Conduct for Kajima Overseas Asia Pte. Ltd. and its subsidiaries and affiliates (collectively and respectively, the "Company") describes the principal understanding of types of threats that exist concerning business information and information systems and the measures which can be taken by all employees of the Company (collectively and respectively, the "Employee") to secure such information and or systems from such threats.

2. Definitions

2.1 Information System

The generic name of a system that provides business related services, including applications and information infrastructures (IT equipment and networks, etc.).

2.2 Information Security ("IS")

To protect the Company's business information and or information systems from theft, loss, leakage, destruction, falsification and the like caused intentionally, by negligence or by natural disaster.

2.3 IS Incidents

The generic name for events that cause or have caused threats to IS.

Example) Leakage, loss, destruction, theft, computer viruses infection, unauthorized access, unauthorized use, and the like of business information.

Loss, destruction, or theft of IT equipment not involving any business information shall be treated as property damage.

2.4 Portable Memory

Portable electromagnetic recording media such as USB memory devices, portable HDDs, printers, MOs, CD-ROMs, DVDs, floppy disks, and the like. Shall include SD card media for mobile phones and digital cameras as well.

2.5 IT Equipment

Servers, PCs, external HDDs, printers, MO drives, CD-ROM drives, smartphones, tablet devices, digital cameras, and the like, which can input, output, save and or record information.

2.6 Social Media (Social Networking Services)

Social networking sites such as Twitter, Facebook, and the like, where various information may easily be exchanged between its respective users.

3. Basic Principal

3.1 Taking or carrying out business information outside from the Company is prohibited. If there is a necessity to do so, follow the rules established less than 6 “Taking Out Business Information from the Company.”

3.2 Use of business information for personal reasons shall be prohibited.

1) Notwithstanding being employed or retired from the Company, personal use of information known through or from business practices shall be prohibited.

2) Business information obtained or prepared shall be, whether personally obtained or prepared, the property of the Company, and its personal use shall be prohibited.

3.3 Personal use of information systems used for business shall be prohibited.

Use of information systems used for business for Internet shopping, Internet auctions, or posting to websites, whether during business hours or not, shall be prohibited.

3.4 Use of business information, information systems, Internet bulletin boards, and or social media, where such act may violate privacy, cause damage to, or cause loss of trust or credit of the Company or its group of companies, shall be prohibited

3.5 Business information (including pictures and video images) and information pertaining to clients is prohibited to be posted on internet forums or social media etc.

3.6 Use of business information and information systems, where such act may violate ethics, morals or the law, shall be prohibited. Especially, extreme care shall be taken to make sure that personal data is not leaked, and to comply with the personal data protection act and other relevant regulations.

4. Management of Business Information

4.1 Segregation Management of Information

1) Business information shall have the segregation of information management clearly defined and shall be treated in accordance thereof. Those without clear segregation defined shall be treated as information confidential to external parties.

2) Segregation management of information shall be defined by the person responsible for IS.

4.2 Access Rights

1) Business information shall be kept and maintained at locations where access is limited to only those related to the information, so that those who do not have authorization to access such information cannot access them, whether intentionally or not.

2) For electronic files, access right shall be provided only to those who have authorization. For electronic files that need advanced information management, encryption and password settings shall be required so that such information may be kept secret in case it may be leaked.

3) For project site offices and the like, since networks may be shared with joint venture partners or subcontractors, access rights restricting users thereto shall be strictly managed to prevent information from leaking to those not concerned.

4) If an employee is relocated or retires, or a part-time employee based on service agreements with external parties or person finish their agreement term, and no longer have necessity to use information systems, their user-rights shall be terminated forthwith.

4.3 Use of Business Information

1) Business information whether on portable memory or on paper shall not be neglected or left unmanaged. Especially at locations such as project site offices, information shall be kept in secure locked locations when leaving or parting from them.

2) Do not leave portable memory connected to IT equipment.

3) Print-outs from printers, copy machines and or fax machines shall not be left printed-out but forthwith picked up.

4.4 Destroying Business Information

1) Destroy business information as soon as it becomes no longer necessary appropriately and without delay.

(a) Portable memory or IT equipment

If recorded data is no longer necessary, delete such data without delay. If portable memory or IT equipment itself is no longer necessary, remove or return them without delay.

In addition, if the portable memory cannot be returned, do not reuse but physically destroy and dispose them after retrieving the data inside.

(b) Paper Information

Business information deemed to have stricter confidentiality than "Confidential" shall be destroyed by shredding or having it destroyed by a secure waste-disposal company. If a vendor shall be appointed due the quantity being large, enter into an agreement with such an external party, which guarantees non-leakage of information and to destroy such paper information by shredding or dissolution, so that such paper information can no longer be read.

2) Information obtained from clients shall be destroyed or returned in accordance with their instructions.

3) If there may be a necessity to carry or take out information, electronic information shall be saved in equipment with security features, and paper information shall be managed and maintained with the segregation of information management clearly defined and marked therein.

5. Management of IT Equipment

5.1 IT Equipment that can be Used

1) IT equipment and portable memory approved by the Company may be used, and the use of personal IT equipment and or portable memory shall be prohibited. In the event personal IT equipment and/or portable storage medium is used under unavoidable circumstances, such user shall follow the internal rules that are provided for separately.

2) Among portable memory, use of non-security featured devices, such as floppy disks, CD-Rs, MOs, DVDs, and the like shall be prohibited, unless otherwise deemed necessary in executing designated works for the client.

5.2 Introduction, Inventory, and Removal of IT Equipment

1) IT equipment or portable memory shall be provided by the Company.

2) Inventory of IT equipment shall be periodically spot-checked to catch loss or theft thereof at an early stage, and completely remove those that are no longer necessary.

5.3 Protection of IT Equipment, etc.

1) High portability equipment, such as note PCs with business information saved thereon, shall be connected with security wires or placed and kept in locked areas or compartments for which physical security may be obtained (such as locked cabinets, etc.) .

2) If IT equipment with business information saved therein shall be taken or carried out, use equipment that encrypts internal data.

3) If business information is saved in PCs, security measures shall be taken for them, including desktop computers, such as by connecting and securing them with security wires at head office departments and project site offices to prevent theft.

4) When newly procuring PCs, procure PCs which have encrypt data capacities as much as possible whether for use inside the Company or not.

5) Do not change settings of IT equipment provided by the Company, other than settings which would strengthen the security thereof (such as password changes, fingerprint authentication, etc.)

6) Inserting memory cards (miniSD, microSD, etc.) to tablet devises is prohibited.

5.4 Measures to be Taken when Incidents Occur

If IT equipment or portable memory with business information saved therein may be lost or stolen, and information has leaked or has a risk of being leaked, such incident shall be treated as an IS incident and measures shall be implemented in accordance with 12 “Measurers to be Taken when Incidents Occur.”

6. Taking Out Business Information from the Company

6.1 If the need to take or carry out business information from the Company arises, obtain prior approval from those responsible for IS.

Example of Carrying Out Business Information

-Presentation and or meetings at client’s office.
-Presenting business data to subcontractors.
-Carrying an emergency contact list for nighttime or weekend troubles.

6.2 Those responsible for IS shall, upon receiving request to take or carry out business information, check the following points and if deemed appropriate, approve such request.

1) Purpose

2) Necessity

(a) Non-necessary information for the purpose is not included therein.

(b) Minimum information will be taken or carried out.

3) Period of information being taken or carried out.

(a) Information taken or carried out shall be returned without delay.

4) Location data is taken to.

5) Security measures.

(a) Use IT equipment or portable memory which has security measures incorporated therein to prevent leakage of information.

(b) If there may be no choice but to use equipment and or devices not described in (a) above, encryption or password protection shall be placed on electronic information which require high level information management.

6.3 Precautions to those taking or carrying out information

1) Beware of theft or loss

(a) Outside of the Company, business information or IT equipment or portable memory with business information saved therein shall not be separated from the body carelessly. (example: placed on shelves of trains or left in parked cars.)

(b) If planned to take abroad, check travel advisories of such country to confirm status of its safety prior to leaving, and take ample anti-theft measures in accordance thereof.

2) Prevention of unauthorized access

Electronic files, such as those strictly confidential with information that requires high level information management, shall be encrypted and password protected, and managed strictly.

3) Prevention of virus infection

(a) When connecting USB memories or similar devices with business information saved therein, confirm that the connecting PC has anti-virus protection.

(b) When connecting IT equipment or portable memory provided by external parties or person to PCs with business information saved therein, confirm that the equipment or memory has anti-virus protection.

(c) In the event you feel that IT equipment or portable recording medium with business information saved therein may have a risk of being infected by viruses, scan and examine them by using anti-virus software without delay.

7. Transaction of Business Information with External Parties or Persons

7.1 When sending faxes or e-mails, make sure that the numbers and or addresses are correct each time to prevent information leakage.

7.2 Use only e-mail addresses provided by the Company when sending out business information. Use of personal e-mail addresses whether receiving or sending out e-mails is prohibited.

7.3 When sending out business information via e-mail, to protect from the risks of interception and miss sending, send it as attachments with encryption and password protection placed thereto. Keep the e-mail texts business information contents to a minimum.

7.4 Transactions of electronic files using the Internet shall follow rules and steps as defined by the Company. If clients request different procedures, confirm that security for such procedure has been obtained, and also obtain prior approval from the Internet Security Development Team ("ISD Team").

7.5 When receiving a questionable or strange email, do not open the link or the file attached thereto and destroy the e-mail in its entirety.

7.6 USB memory devices shall be used when carrying out data and shall be initialized before and after use. When saving data to be presented in portable memory, such as USB memory devices manually test them for virus infections by specifying the device to prevent handing over virus to the receiver of information.

7.7 When physically moving paper or portable memory with business information recorded therein, confirm with those in charge of IS, on how to move such information, and choose the most appropriate way. The following shall be ways to physically move information.

1) Hand carry

2) Send by postal mail or courier service

3) Company's internal courier service (between head office and site office, use of external vendor)

   Although the risk of being sent to wrong addresses are low since it being sent by scheduled delivery by an external vendor, as the carrying bag is a zipper cloth bag, there may be higher risks that the delivery item may be stolen compared to usual courier services, and therefore, is not suitable for strictly confidential information.

4) Registered mail

   Delivery route and status is records from the sender to receiver.

5) Security Delivery Service

   Delivery service with security strengthened, where the receiver is fixed to one person (no substitutes allowed), and location of delivery can be checked via GPS, and the delivery item is place in a locked security box. Since there are many options and prices depending on its security level, choose the one most appropriate for the purpose.

8. Use of Information Systems

8.1 Connection to the Company network of IT equipment is prohibited other than those provided and permitted to be used by the Company.

8.2 Renting or joint use of user IDs and passwords provided to each individual is prohibited.

8.3 Authentication information for information system use shall be strictly managed (such as passwords, etc.)

1) Use passwords that cannot be easily guessed. Examples of passwords not to be used

   - same as user ID
   - fewer than 6 characters
   - repeatedly used same words
   - own name

   Example of Recommended Passwords

   - More than eight characters and include letters, numbers and other special characters.

   If you have no choice but to use only four characters for smartphones, limit the time of mistakes in passwords allowed.

2) Do not maintain or place passwords at places easily visible by others.

3) Do not let anyone else know your password.

4) Change password as soon as you receive the initial password (if system allows such changes. the same shall apply below.)

5) Change passwords periodically.

6) Do not reuse old passwords.

7) If you feel there is a risk that your password has been leaked, change the password without delay.

8) Do not automatically save the passwords, but input the password on every occasion.

8.4 When using a PC, be sure to set the PC in such a manner that the locking mechanism activates whenever leaving or parting from the PC.

8.5 Only use software as approved by the Company, and do not use personal software. Obtain prior approval from the ISD Team for usage of freeware. However, the use of the following software shall be prohibited due to potential security risks involved. (Prohibition of the use)

1) File sharing software (Gnutella, Winny, Share, etc.)
2) Entertainment software (games, etc.)
3) Wall paper (especially those with movement)
4) Mouse pointers, time showing software.

8.6 Use of software versions where support from vendors thereto has been terminated shall be prohibited, due to security updates for such program no longer being offered toward new threats and vulnerability, and measures toward the same not being available.

8.7 Anti-virus software needs to be consistently running and have virus definition files and security patches updated on a regular basis for PCs and tablet devices, etc. (iOS is not mandatory)

8.8 If you feel something is wrong or abnormal with the PC or tablet device, detach them from the network without delay and consult with those responsible for IS or with the ISD Team.

Examples of abnormal behaviors

1) The usual screen does not come up when starting up
2) A strange message appears
3) Data is being changed automatically
4) Data is being broken

9. Measures Against Unintended Copying of Business Information

Visitors and non-project members are prohibited to take photos and use photocopy machines. When there is an appropriate reason, approved personnel who shall wear a strap or arm band as identifications will be allowed to take pictures, after obtaining approval from the person responsible for IS. Concerning photocopies, an employee of the Company shall do so on behalf of the visitor.

10. Measures Against Fraud

Instill and inculcate awareness and a sense of vigilance. Be aware and vigilant to guard against circumstances when the KOA Group may be subject to fraud perpetuated by external parties and adhere to all appropriate measures and protocols implemented by the Company to this effect from time to time.

11. Security Management of Company-provided Cellphones and Smartphones

11.1 Cell phones and Smartphones must be strictly managed to prevent theft and loss.

(1) Do not casually leave them in suit pockets or bags. There have been cases where smartphones have been pick-pocketed from the suit pocket in restaurants and bars when left unattended.

(2) If possible, hang them from your neck using a strap or use a strap that can be clipped or attached to pockets of suits, such as internal breast pockets.

(3) Attach accessories such as bells, so that you will notice it if it falls out.

11.2 Take the following measures for cellphones and smartphones to prevent damage from expanding in case of theft or loss.

(1) Business information saved in its memory, such as SMS, personal e-mail address, data transaction records and or photos, shall be deleted as soon as you finish using them, so that no business information remains in the cellphone or smartphone.

(2) Concerning the SMS and personal e-mail addresses, do not send or forward them between cellphones (smartphones) and the Company e-mail address.

(3) Use of memory cards (miniSD, microSD, etc.) shall be prohibited.

(4) The security lock function shall be activated at all times with a passcode of over 4 digits which is hard to surmise.

(5) The address book is to be kept at a minimum. Do not enter personal data such as home phone numbers and home addresses even if they are a close associate.

(6) The cellphone (smartphone) is to be set so that the phone is locked or data wiped if the passcode is mistakenly input a certain number of times.

(7) For smartphones(and cellphones which may have the function), settings are to be set so that the phone can be located when displaced, and data wiped in case the phone cannot be located.

(8) For smartphones, the most recent security update patch to the operating system is to be applied to the smartphone as soon as it is distributed.

(9) In the event of using a personally owned cellphone or smartphone for business use with the permission of the Company, no business information is to be stored in the phone. Additionally, if the phone is used to access the Company e-mail account, all security measures applied to Company owned cellphones and smartphones must be applied. Detailed regulations for use of a personally owned phone are provided separately.

11.3 In the event of a theft or loss of a cellphone or smartphone, take measures to have the phone locked or data wiped, and contact those responsible for cellphones or the management thereof in your department. If information of clients, neighbors or other parties or person related to business were saved in the cellphone and there may be risks of it being leaked (due to the security lock being switched off, etc.), submit the IS Incident Report (refer to 12. Measurers to be Taken when Incidents Occur, on how to submit the IS incident Report).

12. Entries to head office and other Facilities

12.1 When applicable IDs shall be either worn or carried when inside the facilities.
IDs herein shall mean the following:

1) ID Cards (Employment Identification, etc.)
2) Admission cards or the like provided to external person or parties who visit on a frequent basis.
3) Admission cards or the like provided to visitors on each occasion.

12.2 Measures Against Visitors

Implement measures for visitors based on rules established by each facility.

13. Measurers to be Taken when Incidents Occur

13.1 For head office

1) Forthwith report any knowledge obtained of an IS incident to those responsible for IS.

2) If subcontractors (including group companies) have caused the incident, if such incident occurred under your management, your department shall implement the necessary measures.

3) Those responsible for IS shall report to the ISD Team.

4) Those responsible for IS in the site office shall consult with the ISD Team and implement initial measures and recurrence prevention measures. Depending on necessity, shall report to clients and or internal and or external parties. The ISD Team shall support these measures taken.

13.2 Report Form

1) A report form provided by the ISD Team shall be used for reporting. Try to describe as many details that are able to be obtained at that time for tentative reports and the report prior to its final report.

2) Individuals who caused the incident shall prepare a detailed report and submit the same to the Information Security Administrator (“ISA”).

Supplemental Information

1. Effective Date of Policy
   1) This Policy shall be made effective as of 1 July 2014.
   2) This Policy has been amended as of 12 March 2018
2. Controlling Department

   This Policy shall be controlled by Kajima Overseas Asia Pte. Ltd., Corporate Administration, Headquarters.