Summary of the MROC / Temple Security & Safety Policy

Author: Nicole Casati
Sponsor: Rob Jemmett
Version: 1.0
Last Update: 16 January 2017
Status: Final
File: Summary of the MROC -Temple Security Safety Policy.docx

Table of Contents

1 Principles

- This version provides a summary of the most important provisions for staff at Munich Reinsurance Company of Canada (MROC) and Temple (hereafter referred to as the "Company"). It is not a replacement for the complete contents of the "MROC / TEMPLE Security & Safety Policy" and is not a replacement for the security briefing by the internal contact (for external employees).
- The use of the Company's data, Information and Communication Technology Systems (ICT Systems), premises and office space, operating equipment and machinery, furniture and fixtures, valuables and works of art, or vehicles is permissible only for the purpose of performing the tasks assigned by the Company. The required duty of care must be observed, including that stipulated in these guidelines.

2 Munich Re insurance group Directive on Third Country Data Transfer

- All Staff, must read, understand and comply with the Munich Re reinsurance group Directive on Third Country Data Transfer
- The Directive is a part of our business process. Consideration should be given to how the Directive applies to personal data emanating from an European Economic Area (EEA) country.
- The Regional Data Protection Adviser should be advised immediately of any enquiry or complaint received from a data subject under the Directive.

2.1 Data Protection

- An overriding legal provision, the Personal Information Protection and Electronic Documents Act (PIPEDA) itself or the consent of the affected person is required for the collection, processing and use of personal data. Such activities are otherwise prohibited. Health data is for the most part subject to stricter rules.
- The personal data must be in fact necessary to fulfill the required purpose, and may be made available to others only on a "need to know" basis.
- The data may only be used for another purpose if one of the prerequisites for such use is met, namely overriding statutory regulation, the PIPEDA itself or the consent of the data subject (defined purpose). For example, it is prohibited to use policyholder data received from the Primary Insurance (PI) to compare with applicant data.

- Care must be taken in business processes, and in the selection and design of ICT systems, to use as little personal data as possible (data minimization).
- Contractual provisions on data transfer to other reinsurers/retrocessionaires and clients/cedants must be complied with (e.g. contracts with primary insurers).
- When testing ICT systems, or in training sessions, only fictitious data may generally be used (e.g. no policyholder data).
- The Data Protection Adviser must be promptly informed of any requests by affected data subjects.
- Should an external employee perform any collection, processing or use of personal data with his own ICT resources, or outside the Company's offices, an agreement on contractual data processing must be concluded with him before the contract begins. Otherwise, an undertaking must be signed.
- When forwarding personal data – even within the MR reinsurance group – you should check whether the transmission is permitted under data protection law. This applies both to the sending or making available of files and printouts, as well as, to written or verbal information.

3 Handling of Information

- Information in both digital and non-digital form must be allocated to one of the five confidentiality classes. The class chosen should be a class of which at least one of the potential-loss criteria would apply were unauthorized access to the information to be gained:
  - **C4 Strictly confidential**
    Highly sensitive information intended only for authorized individuals.
  - **C3 Confidential**
    Sensitive information that may be made available to authorized groups of persons.
  - **C2 For internal use only**
    Information that may be made available to authorized groups of people.
  - **C1 For internal use only (Associates)**
    Information that may be made available to all employees and in principle to all external partners and other authorized persons.
  - **C0 Public**
    Information published following an official clearance process.

- The confidentiality classification of a document should be the highest class appropriate for any item of information in the document.
- Appropriate measures must be taken to protect information classified as C3 or C4 from unauthorized access in accordance with the organizational and/or technical circumstances pertaining. This applies particularly to the exchange of such information with persons/systems outside the Company. The connect system, among others, is available for this purpose.
- Class C4 information may be transferred neither to internal nor to external recipients by E-Mail unless adequate safeguards are in place (e.g. encryption).
- Class C3 information should not be transferred to external recipients by E-Mail unless adequate safeguards are in place (e.g. encryption).
- At the moment there is no obligation to label information. If information is labelled, the class designation indicated above should be used.
- Printouts and other paper documents of Class C3 should not, and those of Class C4 must not, be brought to a workplace outside of the Company offices.
- Information in confidentiality classes C1 to C4 may only be stored on ICT systems and electronic storage media in the designated areas (e.g. Worx App on the Corporate Phone) authorized by the Company.
- The storage of data/information relating to our business on local hard disks (e.g. a C-drive) or mobile data media is not permitted.
- Information in confidentiality classes C3 and C4 may not be stored on mobile data media in unencrypted form.
- As a general rule, before information is given over the telephone the identity of the caller and the nature of their request should be confirmed.
- Where workstations are located close to public areas, care should be taken to ensure that information in confidentiality classes C3 and C4 is not accessible from the public area. This means ensuring that documents cannot be stolen, information on screens or flip charts cannot be seen and people are not able to overhear or eavesdrop on conversations.

4 Use of Information and Communication Systems

- Users are responsible for the use of ICT systems and the access to information via their user accounts.
- Installation, modification, removal, de-installation or disposal of ICT devices is to only be carried out by IT staff, or through express instructions provided by IT.
- ICT systems may not be used for the downloading, storage or transfer of offensive or inappropriate material (e.g. pornographic content).
- The circumvention, deactivation or other dilution of safeguards relating to the use of ICT systems is expressly prohibited.
- When leaving their workstation – even for a short time – employees must lock their ICT systems to protect them from use by unauthorized persons.
- Connection of personal or external ICT system or data media to the Company's infrastructure is not permitted without the Company's approval and the express authorization of the responsible Information Security Officer in IT.
- ICT systems that were not made available by the Company may only be used to the extent clearance by the Company has been obtained.
- User IDs may only be used if their use is permitted and they are required for the performance of assigned tasks.
- Use of another person's user ID, even when deputizing for that person, is generally not permitted. It may be allowed in exceptional cases, but must be properly documented.
- Passwords and PINs must be kept secret.
- The automatic forwarding of incoming E-Mails to an E-Mail address not provided by the Company is not permitted.
- Messages clearly recognizable as spam may not be answered, opened or forwarded, and must be deleted immediately.
- Only programs and files supplied to or developed for or by the Company may be used in the ICT systems designated for their use.
- Where files subject to license (e.g. photographs, diagrams, music, videos or programs) are needed for the performance of company tasks and duties, they may only be stored, processed, distributed or used in any other way in accordance with the copyright conditions.

- The use of unauthorized copies of software or data, made available or developed by the Company, is prohibited.

5 Conduct on Company Premises & Facility Protection

- The following applies to keys and IDs with access functions:
  - ☐ they may not feature references to the Company or a particular area
  - ☐ they may neither be reproduced nor provided to third parties
  - ☐ they must be returned to Office Services or the reporting Manager without delay, as soon as they are no longer required for work (e.g. termination, transfer, etc.)
- guests and visitors must be accompanied by a Company employee (usually the host). The latter is to ensure that the visitor respects security rules.
- Dangerous or prohibited items may not be brought onto or stored on the Company's premises unless the Company has given its express permission.
- Objects or ICT devices found (e.g. mobile data media or electronic equipment) may not be used or operated on the Company's premises, and on no account should they be connected to the Company's infrastructure.
- If the ownership/origin of an object found cannot be determined simply, it should be handed in at Reception or to Office Services. If a suspicious object with unknown content is found, the Building Security Desk or Office Services should be informed immediately.
- All work equipment must in any event be returned to the Company on termination of the contract of employment.
- Smoking is prohibited on company premises.
- Open fires and the use of hotplates and portable immersion heaters are prohibited.
- The working of security facilities such as fire and smoke protection devices, extinguishers, alarms, safety instructions/signs and escape and rescue routes may not be impaired or impeded (e.g. by blocking open doors, rendering a device or instructions invisible or removing them), and they must not be obstructed, damaged or misused.
- Non-company electrical or electronic appliances or devices may only be connected to the infrastructure (e.g. electric socket, network socket, telephone connection, USB connection, etc.) with the express approval of IT.

6 Conduct in the Event of a Security Incident & Technical Disruptions

- Anomalies, violations of security or security incidents or any weaknesses identified must be reported to one of the following[i] immediately:
  - ☐ Incidents or suspicions (e.g. suspected virus infection or use of a PC by unauthorized third party) relating to information and the ICT infrastructure: via phone to the Information Security Officer (tel. (416) 359-2175), or to the IT Service Desk via phone (1-877-673-5888) or email to servicedesk-americas@munichre.com
  - ☐ Incidents or suspicions relating to personal data: via phone to the Data Protection Officer (tel. (416) 359-2157), or to the Information Security Officer (tel. (416) 359-2175)
  - ☐ all other incidents or suspicions relating to security: via phone to the Office Services Manager (tel. (416) 359-2193) or to the Building Security Desk (tel. (416) 947-9393)
- Employees should report all technical problems to the IT Service Desk via phone (1-877-673-5888) or email to servicedesk-americans@munichre.com
- The loss or theft of a security card must be reported immediately to Office Services or the Building Security Desk.
- If there is a fire suspected or detected, the Building Security Desk, the Fire Warden or Office Services should be informed immediately.
- In the event of an emergency, upon hearing a continuous fire alarm signal (fast bell), make your way to the nearest exit or fire stairwell immediately. Walk quickly and quietly down the fire stairs and exit the building. Do not use the elevators.
- In the event of an actual or suspected security incident relating to ICT systems:
  - ☐ the ICT system concerned may only continue to be used with the agreement of the Information Security Officer,
  - ☐ only authorized units may take further action (e.g. internal or external communication); the IT Information Security Officer must be contacted prior to action being taken.
- Instructions regarding identification of the cause of the incident, damage limitation or other action to be taken in respect of the security incident should be followed.

7 Document History

Version	Status	Date	Author(s)	Remarks
0.1	Draft	21 November 2016	Nicole Casati	Initial Draft
0.1	Review	09 December 2016	Tracey Anderson	Reviewed and requested document format changes and removal of bold note in section 1
0.2	Draft	12 December 2016	Nicole Casati	Made requested format and content changes.
0.2	Review		Tracey Anderson Jeff Phinney	
0.3	Review	09 January 2017	Jeff Phinney	
0.4	Review	16 January 2017	Nicole Casati	Reviewed document against main document for matching relevance.
1.0	Final	16 January 2017	Tracey Anderson	
1.0	Released			

[i] Further notification channels can be found in the MROC / Temple Security & Safety Policy, in the Appendix, Section 8.1, "Contacts".