Information Technology (IT) Security @ Gen Re

Gen Re®

A Berkshire Hathaway Company

CONTENTS

Gen Re is known for financial security and stability, and for bringing peace of mind to our clients. We keep our promises. It's with the same passion that we want to assure our clients that we take IT security seriously.

Gen Re's robust IT security landscape is not only capable of addressing the ever-evolving security challenges and threats, but at the same time is contributing to the development and deployment of strong IT governance mechanisms. This ensures safe, secure and reliable services to our clients, in accordance with IT industry standards. This document follows (ISC)² CBK, while Gen Re is guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework and its mapping to the International Organization for Standardization (ISO) 27001.

SECURITY AND RISK MANAGEMENT

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Gen Re maintains a business continuity management process that enables us as an organization to continue to manage our business under adverse conditions. This is accomplished through appropriate resilience strategies, recovery objectives, and business continuity plans in collaboration with, and as an integral part of, a risk management function. Gen Re's disaster recovery plan details the restoration of business critical systems, and is updated and rehearsed annually. The processes outlined in our business continuity and disaster recovery plans are designed to ensure that Gen Re can continue to provide services to our clients.

INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT

Gen Re maintains data privacy policies for the United States, Canada and international businesses, which include data security guidelines and controls. Gen Re's Legal department maintains, reviews and publishes these policies. Data Privacy Officers have been appointed in each business platform. Any service providers we use are governed by contractual agreements that are regularly reviewed to ensure compliance with the terms and conditions of the contract.

LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE

Gen Re's IT department takes reasonable steps and applies applicable data privacy policies and procedures to protect personal information and sensitive data. Access management and controls are also used for identification, authentication and authorization to meet business requirements while maintaining confidentiality, integrity and availability.

Authorized users are certified annually and confirm their familiarity with the Gen Re Code of Business Conduct where acceptable use standards are identified. Access to Gen Re data and file servers is restricted to authorized users for support functions. Changes to software configuration and server configuration are governed by a rigorous release management process that requires approval by management before implementation.

The Gen Re Security Incident Management process includes key personnel from various Gen Re organizations to provide identification, investigative services, incident containment, recovery operations and post incident reviews.

SECURITY ASSESSMENT AND TESTING

Gen Re's IT systems and processes are audited internally and externally on a regular basis. Gen Re conducts a technical security assessment of its systems on an annual basis. This assessment attempts to identify exploitable vulnerabilities that, if compromised, could adversely impact the operational and business objectives of Gen Re systems. Gen Re has a comprehensive Security Awareness Program that addresses general and targeted awareness, training employees to improve vigilance, reducing risk and incidents, and testing employees against real-world threats to modify security behaviors.

IDENTITY AND ACCESS MANAGEMENT

User access is requested and granted only for those individuals needing access to the data/system to perform their job functions. All systems require authentication through a unique user ID and password. Our password standard ensures the password is complex. Upon termination, the access is removed for users, vendors and authorized consultants. Regular access reviews are conducted by the business owners and any changes to access proceed through the provisioning system to remove unnecessary access.

ASSET SECURITY

Security controls and procedures are in place to prevent unauthorized access to Gen Re facilities and systems. Access to physical locations is controlled through keycard entry systems. Only those with an operational need are given access. Visitors must adhere to building security protocol based on location.

SECURITY ENGINEERING

Gen Re's IT department follows a software development life cycle that evaluates security architecture and best practices. Detailed risk assessments are conducted for hardware, software and other technology solution providers.

CRYPTOGRAPHY

Cryptographic solutions are used to protect the confidentiality of sensitive information. Transport Layer Security (TLS) and an industry-standard mail encryption solution are utilized. Portable devices (including laptop hard drives, mobile phones and removable storage devices) use NIST approved industry standard cryptography. Digital certificates are used on external websites that provide Gen Re-to-client communication and data transfer facilities.

DATA LOSS PREVENTION

Data loss prevention tools are used to ensure that sensitive information assets in transit are not violating information security policies. Email attack prevention, spam, and website content filtering are also in place. Access to web-based personal email is also blocked and prohibited on corporate computers.

SOFTWARE DEVELOPMENT SECURITY

Application systems are implemented following a formalized software development lifecycle and a quality assurance and change management process. All users must have their own unique user ID and password in order to log on to corporate systems. Regular access reviews are conducted on mission-critical systems, including systems that contain sensitive or financial data, at least annually. Appropriate access rights are defined by information owners based on requirements of business operations.

COMMUNICATION AND NETWORK SECURITY

The Gen Re infrastructure network is segregated logically and physically as operational needs dictate. There are separate environments for development and production. Industry standard anti-virus and encryption solutions are employed within the Gen Re environment. Firewalls are used to prevent intrusion, and monitoring is in place to detect suspicious activity.

SECURITY OPERATIONS

Monitoring is regularly conducted and appropriate action is taken to identify, locate, and investigate unauthorized or suspicious activity. Gen Re uses network behavioral and vulnerability management devices to check the health of the technology environment. In conjunction with threat processing and security information and event management tools, security events are correlated, analyzed and quickly addressed. Gen Re has a thorough incident response plan and team in place should an incident occur.

APPLICATION SPOTLIGHTS

FACWORLD

Gen Re provides FacWorld Life/Health user accounts for clients after each client signs an access agreement form. The clients provide a list of users that require access to Gen Re's FacWorld Life/Health application. Unique user IDs and complex passwords are assigned to each user by Gen Re. The user is required to change the password upon initial login. In Gen Re's FacWorld Life/Health application, clients may securely upload files that are accessible by the clients and Gen Re. All uploaded files are stored securely in a database. FacWorld Life/Health uploads may be classified and segregated based on the nature of the data. All file transfers are automatically deleted after three months.

GEN RE CONNECT

Gen Re provides Gen Re Connect user accounts for clients after each client signs a contract. The clients provide a list of users that require access to Gen Re Connect. Unique user IDs and complex passwords are assigned to each user by Gen Re. Clients are required to accept a license agreement and change their passwords upon first login to Gen Re Connect.

Gen Re

Gen Re delivers reinsurance solutions to companies in all segments of the insurance industry on both a Treaty and Facultative basis. As one of the leading and most experienced reinsurers in the world, Gen Re is represented by a network of more than 40 branch and subsidiary offices in key reinsurance markets.

The difference is…the quality of the promise®

genre.com

IT2022