GREATLAND INFORMATION SECURITY CONTROLS

Greatland has implemented and will maintain an information security program that includes appropriate technical and organizational security measures intended to protect personal information and client confidential information processed by Greatland pursuant to one or more agreements between Greatland Corporation, doing business as Greatland or Nelco Solutions ("**Greatland**") and its customers (collectively, "**Information**"). The measures are adapted to the types of processing activities, scope, context, categories of information, reasonableness of implementation, purposes of the processing and risks of varying probability and severity. Greatland's information security program includes policies and procedures based on the ISO 27001 and NIST SP 800-53 Rev. 4 Framework. Specifically, Greatland implements the following technical and organizational security measures:

1. **Access Control.** Access to systems is governed by Greatland's access control policy. Greatland managers are responsible for requesting employees and approved subcontractor's access rights to systems, applications and information from Greatland's information technology service desk. Greatland's information technology team will grant or deny requests adhering to the access control policy. The access control policy also covers changes and removal of access rights due to role changes or termination of employment. Requests related to access rights follow established processes and are registered in a ticket management system. This enables traceability of the execution including approvals. The access rights related activities (addition, change, removal and review) are carried out by trained staff. Only a limited number of personnel are authorized to carry out these activities. Before granting access to Information or customer systems, Greatland must ensure that its employees and approved subcontractors agree to abide by these information security measures and that employees and approved subcontractors have completed adequate security training commensurate with their role and the sensitivity of the data accessed.

2. **Computers and Servers.** All Greatland computers and servers ("devices"), have antivirus protection software protecting them against computer viruses, spyware and other malicious code. The protection software is managed from a central management console. The console deploys the latest updates of the protection software, sets security policies and actively monitors all devices. Scans of devices are automated and occur mainly in scheduled intervals but are also event-driven. The protection software also scans files when they are opened or otherwise handled by the user, including downloading or uploading of a file to another device. Detected malware is removed automatically when possible and notifications are sent to the central management console for further processing. All Information is stored and processed by Greatland in the United States.

3. **Vulnerability Management.** Vulnerability management covers vulnerability scanning, security updating and penetration testing. Greatland employs a third-party, qualified security company to do monthly scanning of external-facing websites. Greatland performs internal vulnerability scanning of IT infrastructure critical devices twice a year. The central vulnerability management system detects, gathers, classifies and reports vulnerabilities and provides suggestions for remediation. Greatland's vulnerability management system vendor also delivers updates with known vulnerabilities with regular intervals. The vulnerability scans that are scheduled generate a vulnerability report that is analyzed and handled by specially trained personnel. The vulnerabilities are prioritized and remediated based on risk classification. Vulnerabilities that have been remediated are verified through new vulnerabilities scans. Regular security updates are automatically distributed monthly during planned service outages. Security updates that solve critical issues and vulnerabilities are verified at release by trained personnel and distributed with the highest priority. Penetration tests are conducted annually by external parties.

4. **Monitoring.** Greatland security monitors and alarms (active/passive systems) as well as Greatland's external SIEM security partner are fully integrated into Greatland's operations, providing 24×7 security and security teams ready to respond to alerts and events.

5. **Logging.** Logging of activities such as change and removal of users to the Greatland domain, devices

and applications is handled centrally by trained staff. This is done in accordance with regulatory and business needs and requirements. Tasks performed by staff with high authorization are logged. The logs are reviewed with a risk-based perspective. Identified deviations are followed up and, when applicable, escalated as incidents. The systems logs are protected against removal and manipulation. This is to ensure its integrity, confidentiality and accuracy. Deletion occurs in accordance with applicable legislation.

6. **Encryption.** Sensitive Information (including all sensitive personal information and information designated by customer as confidential) is encrypted during transmission using up-to-date versions of TLS 1.2+ or other security protocols using strong encryption algorithms and keys. Sensitive Information is also encrypted at rest within the system.

7. **Backups.** Data backup is automated and carried out according to a documented schedule. The backup solution used by Greatland is redundant and backup media is stored at a different physical location. Alarm triggers are set on backup jobs to detect and report deviations and incidents.

8. **Disaster Recovery.** Greatland maintains a disaster recovery plan to ensure that Greatland services remain available or are recoverable in the case of a disaster. This is accomplished through building a robust technical environment including redundancy between our facilities. Testing is completed annually.

9. **Oversight.** Greatland's information security program is governed by a committee that meets quarterly to discuss information security issues. Greatland also performs an annual SOC II audit that assesses the effectiveness of our information security program.

10. **Cyber Insurance.** Greatland maintains cyber liability insurance or a similar insurance product that insures liability for privacy, data, and network exposures.

Last Modified: May 19, 2021
Last Reviewed: September 30, 2024