NOTARYGO
NATIONWIDE SIGNING SOLUTIONS

NotaryGO, Inc.
Privacy Program

Jeff Stone
Mike Song
Erica Cornejo
2019

19 06-18

Purpose
The intent of this document is to specify NotaryGO Inc. Privacy program, inclusive of information handling, metrics, risk management and monitoring program.

General

- All employees, contractors and members of NotaryGO, Inc. workforce must guard against improper use or disclosure of NotaryGO clients' or participant's information.
- All employees are required to be aware of their protocol and security responsibility under NotaryGO privacy policies
- All NotaryGO employees must take security awareness training and annual continual training during their employment with NotaryGO.
- Supervisors are responsible for assuring that employees who have access to confidential client information, whether it is electronic, hard copy, or orally, are informed of their responsibilities.
- NotaryGO employees who violate NotaryGO's policies and procedure regarding the safeguarding of client information are subject to disciplinary action by NotaryGO, Inc. up to and including immediate dismissal from employment and legal action.

Information Handling

- Life cycle of client information is in four stages –

Collection > Maintenance > Use > Disposition

- Collection of information is to be done through secure means - e.g. encrypted e-mail or secure https download by account supervisor.
- Maintenance of information is to prepare then deliver document/ information as an encrypted (128 bit RC4 technology) document to Signing Agent.
- Signing Agent will print, notarize, and then return the required document to the intended party via FedEx.
- Dispose any residual digital information after the signing is complete. Dispose any hard copy immediately into a secure shredding bin.
- All, if any, backup media that may retain secure client information will have a life cycle of 4 working weeks. After 4 weeks, it is formatted for next life cycle, rendering all previous private, secure information unusable.

Security Account practice

- Administrator and security accounts with privileged access are not shared among other users.
- User passwords are reset after 90 days, and must adhere to strong password policy:
    - Include both upper and lower case letters
    - Include 1 or more numerical digits
    - Password length more than 6 characters
    - Cannot re-use previous 3 passwords

Non Public information (NPI)

- Non public information is any personal identifiable data which cannot be obtained publicly. Example – full name and address, financial information (e.g. account numbers, social security number, financial account numbers, etc.
- All NPI data is to be handled with security in mind, and only visible when data is needed by the appropriate personnel
- Network and software security group plus event logs will be used to control proper access and log user actions on NPI data

Metrics

Metrics for NotaryGO is measured by the following Key Performance Indicators:

- Technical intrusion
- Break in Information Chain of custody
- Loss of information (document, attachment, email, etc.)
- Theft

In response to any of the above incidents, top level Operation and IT executives will be immediately informed to take necessary actions. Affected stakeholder(s) will be informed after risk assessment, followed by necessary risk mitigation will take place.

President – Jeff Stone

IT Director – Mike Song

HR Manager – Erica Cornejo

Please email or call for any questions. contact@notarygo.com | (855) 204-1204

Risk Management

Risk Management is a management responsibility. Below are the key roles of the personnel who will support and participate in the risk management process.

Senior management must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. Senior Management must also assess and incorporate results of the risk assessment activity in the decision making process.

IT Security Practitioner(s)
IT security practitioners (e.g. network, system, application, email, and database administrators) are responsible for proper implementation of security requirements in the IT systems. As changes occur in the existing IT system environment, IT security practitioners must support or use the risk management process to identify and safeguard IT system as a whole.

HR Management
NotaryGO's personnel will be properly informed with up to date Risk Management's key points and their responsibility. Trainings will be conducted as needed. All related materials will be readily available to NotaryGO's workforce.

Assessment > Mitigation > Evaluation of Risk Management

Assessment
Risk level Matrix: High (50 to 100) Medium (10 to 50) Low (1 to 10)

Threat Likelihood	Impact		
	Low	Medium	High
High (1.0)	Low 10x1.0 = 10	Medium 50x1.0 = 50	High 100x1.0 = 100
Medium (0.5)	Low 10x0.5 = 5	Medium 50x0.5 = 25	Medium 100x0.5 = 50
Low (0.1)	Low 10x0.1 = 1	Low 50x0.1 = 5	Low 100x0.1 =10

Rating of High, Medium, and Low, represents the degree of level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management must take for each risk level

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is assessed as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.

Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is assessed as low risk, the Management and IT security officer must determine whether corrective actions are required.

Mitigation
Risk mitigation involves prioritizing, evaluating and implementing the appropriate risk reducing controls.
IT preventative controls

- Authentication – The authentication control provides the means of verifying the identity. Mechanisms include: password, PIN, using strong authentication (e.g. token, and Kerberos).
- Authorization – The authorization control enables granular access to allowed resource.
- Protected Communication – The protected communication controls ensure the integrity, and confidentiality of sensitive and critical information. Protected communication sue data encryption method (e.g. VPN, IPSEC, DES, 3DES, RASS, MD4, and secure hash) to minimize network threat.
- Backup scheme, logs and Anti-Virus program will be utilized to bring IT system and information to an acceptable system state.

Management Controls
Management security controls are implemented in conjunction with technical controls.
Detection management controls –

- Implement personnel security controls, including personnel clearance, background checks, rotation of duties
- Periodic review of security controls to ensure that the controls are effective and are in practice
- Provide continuity of support and develop, test, and maintain the continuity of operation.
- Establish incident response capability to prepare for, recognize, report and respond to incidents.

Incident response Team:
Jeff Stone - Management
Mike Song – IT System
Erica Cornejo - Operation

Please email or call for any questions. contact@notarygo.com | (855) 204-1204

Risk Evaluation

- NotaryGO will conduct annual risk evaluation.
- Senior management and IT team will apply risk assessment methodology to an operation and system risk controls.
- Cost effective safeguards will be applied as needed.
- The awareness and cooperation of members of the user community will be enforced by supervisors.

Monitoring and Logs

System Logs – Windows event logger logs all mission critical transactions. Retention period is 5 working weeks. Logs are reviewed monthly **
Firewall Logs – Organization to internet protocols a logged via firewall. Retention period is 5 working weeks. Logs are reviewed monthly**
MS Exchange – email transactions are logged by MS mail server. Retention period is 5 working weeks. **

** Information on backup media is rendered unusable when formatted for next backup cycle - 4 weeks. Native logs are weekly written over.

Security and Incident Awareness:

Personal Information is data that can be used to identify an individual and potentially harm homeowners, clients, or associates if lost, disclosed or inappropriately modified.

Security Incident is a situation (physical or electronic), whether suspected or proven, deliberate or inadvertent, that threatens the integrity, availability or confidentiality of personal information

Security Awareness training, certification of completion and annual training are mandatory for all employees of NotaryGO.

Information Security – Data and Information is hosted in 1st Tier SSAE 16 Certified Datacenter. Physical and Technical controls are in place to protect and monitor all data managed by NotaryGO

Signing Agent checklist:

Information handling -
Print only the document(s) to be notarized, and if needed borrower's copy.
If excess document exists, it is to be destroyed or properly shredded immediately.
No electronic copy is to be saved anywhere.

All digital foot prints of the document is to be erased – IE cookies, emails, attachments and https address(es)

Security Requirements -
Following Antivirus software vendors are approved by NotaryGO, Inc:
Avast, GFI, Norton, McAfee, or Trend w/ latest definition and program engine.

Timed Logout –
NotaryGO's Web session has an idle session limit of 15 minutes. Afterwards, the session will close, logout, and requires login credential to continue.

Incident Response:
Upon any incident(s) out of norm of information handling, please contact NotaryGO, Inc. immediately.
(855) 204-1204
info@NotaryGO.com

Please call NotaryGO, Inc. for any questions. (855) 204-1204

Incident Management Procedure:
Incident response Team:
Management
Jeff Stone
Systems
Mike Song – Director of IT
Operation
Erica Cornejo – HR/ Accounting
Bridget Ziemann – Locating Division Manager

Please email or call for any questions. contact@notarygo.com | (855) 204-1204

The goal of the incident response team is to maintain business continuity and defend against future threats.

Training and Awareness:
- Train NotaryGO employees, affiliates, and Signing Agents on Information Protection and Privacy issues
- Define public, personal, confidential and secrete information for electronic and non-electronic forms
- Publish Incident Response Team's contact information

Procedure

1. Document Event(s)
    a. Date and time
    b. Who or what reported the event
    c. Detailed description of the event
    d. Identification of the host(s) that the event is related to. Electronic and non-electronic information.
2. Assign Event to an Incident Identifier
3. Assign severity level to Incident – Low, Medium, or High
4. Assign the Incident to a Handler
5. Notify and inform impacted parties including Clients and or Lenders
6. Contain and Eradicate.
7. Update impacted parties
8. Create follow-up report

Store Incident File for record.