Table of Contents

1. Scope of Policy

1.1. Personnel

This policy applies to all IGEL employee and contractors (“Personnel”) with access to company information and systems.

1.2. Systems

This policy applies to all IGEL corporate systems and systems that provide services to customers.

1.3. Jurisdictions

This policy applies to all IGEL entities and jurisdictions involved. The policy is subject to local legislation. When the local law is more, or less, restrictive than this policy, the stricter rule prevails. Any waivers from the policy must be reported and recorded with IGEL’s Legal & Compliance function.

2. Personnel Security Policies

2.1. Employment and Information Security[1]

2.1.1. Employee Background Check

All employees are required to submit to a background check and provide specific documents verifying identity at the time of employment. Failure to cooperate fully with the background check process or any dishonest or omissions in the information provided may preclude employment with IGEL. Background checks differ by geography to account for local laws. Depending on the jurisdiction, this may include criminal checks, citizenship check, education and employment history. All background checks for U.S. employees comply with the Fair Credit Reporting Act. Background checks are performed by a reputable third-party vendor.

2.1.2. Employee Background Check Rescreening

If an IGEL Customer requests the rescreening of an employee working on that Customer’s account, HR will evaluate whether to honor the request and at its sole discretion rescreen that employee, which may be dependent on local regulations. An employee may only be rescreened once under this provision.

[1] ISO A.7.1, A.7.2.1, A.7.3

2.1.3. Confidentiality and NDA

All personnel must sign the IGEL confidentiality agreement (NDA) upon hire. Upon termination, employees are reminded of their obligations under the IGEL NDA.

2.1.4. Attest and Follow All IGEL Policies

All employees must read and acknowledge they have read and will abide by the Employee Handbook and Information Security Policy (once finalized), both of which describe employee responsibilities and policies for information security and confidentiality. Employees must follow these policies and related standards and to cooperate with Security during audits, investigations and incident response. These policies will also be available on the HR portal.

2.1.5. Reporting Security Incidents

All personnel must report known or suspicious security/privacy issues, violations and breaches to Security by emailing it-support@igel.com.

2.2. Security Training[2]

2.2.1. Annual Security Awareness Training[3]

2.2.1.1. All new hires must complete IGEL's security awareness training to protect the human element of security at IGEL. Enforcement of mandatory annual security training for all employees will be implemented in 2020.

2.2.1.2. This training is developed by the Security and Compliance departments.

2.2.1.3. The training shall consist of relevant security topics accounting for current security trends, human vulnerability landscape and IGEL's latest risk assessment.

2.2.1.4. Training shall be coordinated with the HR, Security or Compliance departments to ensure proper administration and compliance.

2.2.1.5. Training shall be reviewed annually and updated as needed by Security and Compliance

2.2.1.6. Records of training completion must be collected and retained for at least one year.[4]

2.2.2. General Security Awareness Training

2.2.2.1. An ongoing security awareness program must be presented to all employees. This program may consist of regular correspondence

[2] ISO A.7.2.2, NIST AT-1
[3] NIST AT-2
[4] NIST AT-4

via e-mail, supplemental seminars, training and other methods to maintain security awareness among employees.

2.2.3. Role-Based Security Training[5]

2.2.3.1. Role-based security training shall be developed and administered to personnel as determined by Security and Compliance based on security risk or when required by information system changes as noted in the Role-Based Security Training Plan, which shall be finalized in 2020.

2.3. Password Security

2.3.1. Applicability

- These password requirements apply to all IGEL corporate and production networks and data.

2.3.2. Password Strength Requirements

- Minimum of 8 characters, 15 characters highly recommended.
- Minimum complexity (3 out of 4): uppercase, lowercase, numeric and non-alphanumeric
- Must be changed at maximum every 90 days
- Must not use previous 3 passwords

2.3.3. Password Protection Standards

- Do not share your passwords with anyone.
- Do not repeat passwords for any work or personal accounts.
- Do not reveal passwords over the phone, via email or in any shared online portal or files.

2.4. Acceptable Use[6]

2.4.1. Use of Company Systems

The purpose of this Acceptable Use Policy is not to impose restrictions that are contrary to IGEL's established culture of openness, trust and integrity. Rather, this policy's purpose is to protect IGEL's employees, customers, partners, and the company from illegal or damaging actions. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, are the property of IGEL. These systems are to be used for business purposes in

[5] NIST AT-3

[6] ISO A.12.5, A.12.6.2

serving the interests of the company, and of our clients and customers in the course of normal operations.

While limited personal use of IGEL networks is acceptable and IGEL desires to provide a reasonable level of privacy, users should be aware that the data they create on IGEL systems remains the property of IGEL and is subject to the same monitoring and scrutiny.

Effective security is a team effort involving the participation and support of every IGEL employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

- All data created, stored and transmitted on IGEL information systems are the property of the company.
- System use and activities may be monitored, information may be examined, and if required deleted or intercepted.
- IGEL systems must be accessed and managed only by IGEL personnel.
- Business conducted on company information systems must adhere to all company policies.
- While not targeted for examination, personal activity on IGEL systems is subject to the same level of examination as business activity.

2.4.2. Unacceptable Use

The following activities are in general prohibited. Personnel may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems admin disabling network access of a host if it is disrupting production services).

Under no circumstances is any IGEL personnel authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing IGEL information networks systems or resources.

The following activities are strictly prohibited:

Intellectual Property Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the

installation or distribution of "pirated" or other software products that are not appropriately licensed for use by IGEL.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which IGEL or the end user does not have an active license.
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.

Information Security Activities

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to IGEL IT is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Confidentiality

- Providing information about, or lists of, IGEL employees to parties outside IGEL.
- Transmission of IGEL Confidential Information via unencrypted end user technologies or third-party providers not procured by the Company (e.g. non-IGEL procured email, backup, file synchronization and file collaboration utilities).
- When using remote access, copying IGEL Customer data to local storage or removal media

E-Mail/Communications

- Using an IGEL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Subject to local laws and regulations, creating, using or distributing any disruptive or offensive messages, including offensive comments about race, gender, gender expression, hair style, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any IGEL employee should report the matter to their supervisor immediately.
- Any form of harassment via email, telephone, or messaging, whether through language, frequency, or size of messages.
- Making fraudulent offers of products, items, or services originating from any IGEL account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within IGEL's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by IGEL or connected via IGEL's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups or forums or message boards (newsgroup spam).

2.5. Approved Software

2.5.1. Approved Software Guidelines

Laptops, workstations and associated software are provided by the Company to employees. Only approved software may be used on Company systems and commercial software may only be installed with a valid license.

Operating systems and common business applications approved for Company use are managed by IT and distributed or approved for manual installation by IT to corporate users. Users that need additional application/services must contact IT to request the software. IT will either:

- Purchase and provide the application to the user, retain the source/media, and control the license
- Direct the user to purchase the application with funds from the requesting department, provides such use does not violate any other company policy
- Forbid the use of the application on Company systems for reasons including (but not limited to): incompatibility with current systems or unacceptable security risk exposure

2.5.2. Prohibited Software

Any software not expressly approved by IT is prohibited. The following list includes expressly prohibited software:

- Peer-to-peer file sharing network clients including but not limited to: BitTorrent, eDonkey, and Gnutella/Limewire
- Bitcoin or other cryptocurrency mining software
- Applications that subvert firewall and VPN security measures, such as GoToMyPC, LogMeIn, Hamachi, etc.
- Software tools for cracking passwords, sniffing networks, creating malicious software and compromising or controlling other systems, unless required by the user’s job duties.

2.5.3. User Software Responsibilities

Users are responsible for a reasonable level of care to ensure that their Company-owned systems comply with this policy. User responsibilities include:

- Not installing unapproved or prohibited software on company systems, regardless of the licensing or source of funds
- Not installing company software on personally owned devices, unless specifically permitted by IT

- Not disabling protective software such as anti-virus scanners, monitoring software, or firewalls
- Verifying computer backup, encryption, and automatic system update programs run properly and regularly
- Connecting Company-issued systems to the Company network frequently to obtain updates and provide monitoring data, as applicable

2.5.4. Anti-Virus Software Guidelines

All Company workstations and laptops must have IGEL's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into IGEL's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the IGEL Acceptable Use Policy.

2.6. E-mail Security[7]

2.6.1. Email Security Technology

IGEL employs information security safeguards to maintain a secure corporate e-mail system.

2.6.2. Phishing Emails

IGEL personnel should never open any links, files or macros attached to an email from an unknown, suspicious or untrustworthy source or unexpected email. Report any suspicious emails by forwarding them to it-support@igel.com.

2.6.3. External E-Mail Forwarding

Employees must exercise utmost caution when sending any email from inside IGEL to an outside network. Unless approved by an employee's manager or IGEL IT, IGEL email will not be automatically forwarded to an external destination. Sensitive information will not be forwarded.

2.7. Workspace Security

2.7.1. Clean Desk Policy

When away from their workspace for an extended period or at the end of the workday, personnel must:

- Clear their workspace of all IGEL-related data (papers, physical media, etc.)

[7] ISO A.13.2.3

  - ○ If in doubt, throw it out or shred confidential/sensitive documents.
- Store IGEL laptops or physical media containing Confidential or Sensitive Information in a locked drawer.
  - ○

2.7.2. Workstation Security

- Lock your screen when you leave your laptop or workstation for any period of time. Do not assume the automatic screensaver will activate to protect your system.
- Do not post confidential or sensitive information on walls, bulletin boards or make it readily available at your workspace (e.g. binder on your desk, passwords written on post-it notes on your desk, etc.).
- Request and install a privacy screen if you frequently work with confidential or sensitive information.
- Restrict physical access to your workstation only to authorized personnel.
- Clean whiteboards in public areas at the end of meetings.

2.7.3. Remote Workspace[8]

Personnel working remotely must follow all of the above workspace security policies along with the following:

- Ensure that only authorized personnel have access to IGEL related systems and information (i.e. restrict access from non-IGEL personnel including family, friends, workers, delivery people, etc.)
- If at home or on the road, use a secure WiFi connection (at least WPA2 encryption) to access IGEL systems

2.8. Physical Security[9]

2.8.1. Access

2.8.1.1. All access points to the main entrance of an IGEL office requires a key or badge, access PIN, or security guard access.

2.8.1.2. Keys and badges are issued at the beginning of employment and must be returned or deactivated at termination of employment.

2.8.1.3. Issuance and return of keys and badges are tracked and documented for each employee.

2.8.2. Monitoring (IGEL HQ)

2.8.2.1. All access points to an IGEL HQ have CCTV monitoring and recording 24/7.

[8] ISO A.6.2.2

[9] ISO A.11

2.8.2.2. Subject to local laws and regulations CCTV recordings are reviewed on an as-needed basis.

2.9. Visitor Access

2.9.1. Visitor Check-In

2.9.1.1. All visitors must sign a NDA and wear a visitor's badge before entering the main office area. (This provision will be implemented in 2020.)

2.9.1.2. All visitors must be met by their employee sponsor at check-in and be accompanied by their sponsor at all times.

2.9.1.3. A visitor cannot sponsor another visitor.

2.9.1.4. Visitors who do not have official business with IGEL (e.g. friends or family) may be restricted from prolonged visits and may be required to stay in the common reception area.

2.9.2. Photographs and Cameras

2.9.2.1. Visitors are not permitted to take photographs inside of IGEL premises, unless approved by the sponsor's department head.

2.9.2.2. Dedicated cameras are not permitted onsite. Smartphones, tablets, and computers equipped with cameras are permitted.

2.9.3. Information Disclosure

2.9.3.1. Visitors should not request information that does not pertain to their visit or work being performed.

2.9.3.2. Individual department heads may impose additional restrictions, which are considered appropriate to the successful operation of the individual team or visitors in the workplace. The company reserves its right in its sole discretion to deny authorization to a visitor for any reason including, but not limited to, the requested guest or visitor has been disruptive in the past, there is a special event scheduled on the date(s) requested, or the work environment is not appropriate for the visitor or guest due to safety or other reasons.

2.9.4. Exit Inspection

2.9.4.1. Visitors may be subject to a brief search of their bag or other luggage as they exit the premises.

2.9.4.2. Permission for this search is granted by the Visitor signature in the NDA/Visitor Agreement Form.

2.9.5. **Data Center Physical and Environmental Security**[10]

2.9.5.1. All physical and environmental protection policies, procedures and systems for IGEL's data centers are managed and controlled by IGEL's data center providers.

[10] NIST PE-1

2.9.5.2. These physical and environmental protections include: physical access authorization, physical access control, monitoring physical access, visitor access records, emergency lighting, fire protection, temperature and humidity controls, water damage protection, and delivery and removal.

2.10. Mobile Device Security[11]

2.10.1. BYOD Policy

Except for North America, IGEL has a Choose Your Device ("COYD") Policy where IGEL provides the employee with an IGEL issued smartphone and/or tablet that is owned by IGEL and managed and controlled by IGEL IT via an MDM solution.

In North America, IGEL has a Bring Your Own Device ("BYOD") policy with respect to smartphones and tablets. IGEL employees may use an approved BYOD device to access IGEL network and systems subject to these and all other Company policies.

2.10.2. Mobile Device Management

- Mobile devices that connect to Company networks and applications (email, VPN, instant messaging, etc.) must be approved by IGEL IT and conform to IGEL issued MDM policy.
- Mobile devices must use either the current or one version behind the current iOS operating system.
  - Users must upgrade their mobile operating system within two weeks of its release by Apple.
  - Users may not modify the device vendor's provided operating system code or functionality (e.g. Jailbreak or root the device)
- Mobile devices may be required to download and install management and security tools and configuration files.
- Mobile devices must use only approved applications from the device vendor's application store (i.e., Apple App Store).
- Mobile devices must be expunged of all Company data when the user leaves the Company.
- Users are responsible for protection of a mobile device with access to Company systems and must take reasonable precautions to prevent loss and theft.
- Users must immediately report to IT any theft, loss or transfer of ownership (if applicable) of a mobile device with access to Company systems.

[11] ISO A.6.2.1, NIST AC-19

- Mobile devices and uses determined to be out of compliance with Information Security policies or present a threat to IGEL are subject to Company Data destruction and deactivation from Company network access.

2.10.3. Mobile Device Data Standards

- Must be configured to encrypt resident data at rest.
- Must be configured to require a password or passcode for use/unlock.

2.10.4. Mobile Device Data Treatment

- Users must not access, store or share Company data using unauthorized application or services, including use of personal accounts on hosted services (e.g. personal Google Apps, etc.)
- Backups of mobile devices with access to Company data may only use the device vendor's primary backup service, such as Apple's iTunes/iCloud or other IGEL IT approved solutions.

2.11. Remote Access[12]

IGEL personnel with remote access privileges to IGEL systems must ensure their remote access connection maintains the same level of security as the user's on-site connection at IGEL offices.

2.11.1. Secure remote access must be strictly controlled. Control will be enforced via authentication or public/private keys with strong passphrases.

2.11.2. IGEL personnel with remote access privileges must ensure that their IGEL-owned which is remotely connected to IGEL's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

2.11.3. All hosts that are connected to IGEL internal networks via remote access technologies must use the most up-to-date anti-virus software. Third party connections must comply with requirements as stated in the Third Party Agreement.

2.11.4. Organizations or individuals who wish to implement non-standard Remote Access solutions to the IGEL production network must obtain prior approval from IGEL IT.

2.12. Customer Data Security

2.12.1. IGEL Products and Services Do Not Collect Customer Data

IGEL products and services do not collect, process, or transmit Customer Data. The provisions in this section are established in the event Customer Data is collected or processed by IGEL.

[12] NIST AC-17

2.12.2. Definition of Customer Data

Customer Data is personally identifiable information (“PII”) from Customer or Customer Confidential Information provided by the Customer to IGEL as part of IGEL’s performance of its Services.

2.12.3. Customer Data Custody and Management

Customer Data must be restricted to authorized environments. Only IGEL employees that require Customer Data access as part of their duties shall be granted access on a principle of least privilege basis.

2.12.4. Sensitive Data Handling Policy

IGEL must protect internal corporate and Customer Data from loss or exposure to avoid reputation damage or the appearance of impropriety along with other adverse impacts to IGEL and our customers. The following serves as the data handling policy for all sensitive data which includes Customer Data.

2.12.4.1. Scope of Policy

This policy applies to any employee, contractor, or intern with access to sensitive data.

2.12.4.2. Role Based Access

You will receive access to sensitive data restricted to the access necessary for you to conduct your job functions.

- Additional role-based access may be assigned by your manager with approval from Security and IT.
- Exceptions to individual access assignment may be requested in accordance with the Exceptions policy (InfoSec Policy Section 6).

2.12.4.3. Need to Know Access

You may only access Customer Data to the extent necessary to fulfill your job responsibilities at IGEL. Any Customer Data access outside the scope of a specific job function or task is a violation of this policy.

Examples of Acceptable Use

- Accessing customer data for product improvement research
- Accessing customer data for customer support

Examples of Unacceptable Use

- Accessing data to gain competitive intelligence
- Accessing data to gain non-public business information
- Accessing data for any purpose not clearly linked to a business purpose

2.12.4.4. Monitoring

IGEL holds the right to monitor, log and audit all data access, up to and including Customer Data access.

2.12.4.5. Training

If applicable, Personnel must complete sensitive data training prior to receiving sensitive data access. If you already have sensitive data access, you must complete the training within 30 days of its release. sensitive data Access training may be incorporated into other training such as Annual Security Awareness Training.

2.12.4.6. Penalties

Violation of any of the requirements of this policy and applicable standards by will result in suitable disciplinary action, up to and including termination and referral to law enforcement, if applicable.

2.12.5. Storage and Transfer of Customer Data

2.12.5.1. Customer Data may not be stored or transferred on unencrypted removable media

2.12.5.2. Customer Data returned to the Customer from IGEL systems must be transmitted via encrypted files or links, following the encryption standard.

2.13. Media Security and Disposal[13]

2.13.1. Paper-based media

Paper documents, notebooks, brochures and similar items classified as Confidential or Sensitive must be disposed by shredding or a certified shredding service.

2.13.2. Corporate Data Disposal (will be implemented in 2020)

2.13.2.1. Technology Equipment Disposal

2.13.2.1.1. When technology assets reach the end of their useful life they should be sent to the local IT office for proper disposal.

2.13.2.1.2. IT will destroy or securely erase all storage mediums in accordance with current industry best practices.

2.13.2.1.3. Any equipment not in working order will be donated or disposed of according to current environmental guidelines.

2.13.2.1.4. Prior to leaving IGEL premises, all equipment must be removed from the Information Technology inventory system.

2.13.2.2. Corporate Smartphones/Other Devices

[13] ISO A.8.2.3, A.8.3

Erase data using available data security features in the device manufacturer’s management software (e.g. iOS) before they are returned or redeployed.

3. Technical Security Policies

3.1. Access Control[14]

3.1.1. Principle of Least Privilege

Information systems and application access must be granted on a least privilege required basis. The set of access privileges granted to a user must be no more than that required to perform the job responsibilities as described by the user’s job description or contract agreement.

3.1.2. User Access Control

3.1.2.1. General

3.1.2.1.1. Access to all company systems and applications shall be controlled by a secure logon procedure.

3.1.2.1.2. Failed login notifications must not indicate the nature of the failure.

3.1.2.1.3. Networks must implement routing controls based on positive source and destination address.

3.1.2.2. User Account Responsibilities

3.1.2.2.1. User access is restricted to that user. Users are prohibited from sharing access with, divulging passwords to, or requesting passwords from any person for any systems or applications.

3.1.2.2.2. If a user receives credentials from another user, they must report it to Security within one business day.

3.1.2.3. New User Accounts

3.1.2.3.1. Each user account must have a unique username/password combination for access.

3.1.2.3.2. For new employees, subject to local law and regulations, HR is responsible for verifying that background checks and confidentiality agreements are concluded acceptably and to notify IT to create user accounts with basis user privileges.

[14] ISO A.9

3.1.2.4. Account Changes, Transfers and Terminations[15]

3.1.2.4.1. Account changes must also maintain the least-privileges required including granting or revoking privilege due to user change in status, transfer or termination.

3.1.2.4.2. Account terminations are required by the end of the business day for voluntary user terminations. Immediate account termination may be applied in the event of involuntary termination. Upon termination, all IGEL physical assets must also be collected.

3.1.2.4.3. Account transfers where prior access must be disabled and revoked and new access provisioned must occur within 5 business days of the transfer.

3.1.2.4.4. In the case of an account transfer or termination, all information, data access and resources formally controlled by the transferred staff must be retained by another authorized staff member.

3.1.2.5. Account Change Responsibilities

3.1.2.5.1. Account access change process is managed by IT.

3.1.2.5.2. User’s manager is responsible for notifying IT to request user access changes in the case of a change of user duties or transfer.

3.1.2.5.3. User’s manager is responsible for notifying IT in case of user termination.

3.1.2.5.4. IT is responsible for routing access request cases to corporate system owners (or their designees) for approval, making account changes, and tracking changes.

3.1.2.5.5. System owners are responsible for reviewing account changes.

3.1.2.6. Access Review

3.1.2.6.1. System and application owners must review account privileges to verify appropriate levels of access.

3.1.2.6.2. System and application owners are responsible to identify and change account privileges as required (e.g., user terminated or other change in status and access requirements).

3.1.2.7. Network Security Access Management

3.1.2.7.1. IT manages and controls IGEL’s corporate network and works with Security to protect and secure information systems and applications.

[15] NIST PS-4, PS-5, ARCA-006

3.1.2.7.2. Security maintains and manages the security of all IGEL networks via network security technology (e.g. segregation of networks, VLANs, etc.), configuring technical parameters (e.g. secure authentication) and access restriction mechanisms (e.g., firewalls).

3.1.2.7.3. Distinct groups of information services, users, and information systems will be segregated within IGEL's network environment.

3.1.2.8. Source Code Access

3.1.2.8.1. Authorization of access to source code must follow the requirements of this access control policy and segregation of duties policy.

3.1.2.8.2. Source code must be managed according to defined procedures and stored in a secure environment.

3.1.2.8.3. Source code repositories must be segregated into logical functional groups such that no single user has access to all code under any organization or group control.

3.1.2.8.4. For sensitive source code containing trade secrets, the repository should have access restricted to those individuals working on the code, auditing the code, reviewing the code, and testing the code.

3.1.2.8.5. Outbound electronic communications must be monitored to identify leakage of code.

3.1.2.8.6. Outsourced software development must be managed following the requirements in this information security policy.

3.1.2.9. Administrator Access

3.1.2.9.1. Root access must be limited to console sessions, after first logging in under the individual user account.

3.1.2.9.2. When an administrator (system, network or database admin) is transferred or terminated, that employee's manager is responsible to ensure that user's account is locked and the corresponding password(s) for administrative access are changed the same business day.

3.1.2.9.3. Production system access control must include network-limited access, and multiple points of authentication. Production system authorization requires the approval of the Chief Technology Officer or their designee.

3.1.2.10. Permitted Actions without Identification or Authentication[16]

[16] NIST AC-14

There are no permitted actions on IGEL systems without identification or authentication.

3.2. Segregation of Duties

3.2.1. Development and Production software must run on systems that are physically and logically separate.

3.2.2. Logical and physical access to development, quality assurance, release engineering, production, and corporate systems must be segregated appropriately according to job duties.

3.2.3. Administrative access to Production for a non-production team employee requires the approval of the IT management or their designee.

3.2.4. Read-only access to monitoring systems and logs not containing Customer Data must be approved by the respective system owner.

3.2.5. Scripts and other utilities must not store administrative-level passwords in clear text. Scripts that require such access should run interactively, such that an authorized person must enter the administrative password from an authenticated login.

3.3. Change Management[17]

Changes to information systems (other than routine administrative activities) must be managed by a change control process that includes the following elements:

- Identification of information system changes
- Assessment of potential impacts, including security risks, of such changes
- Planning and testing of changes, including version control of code and configurations
- Communication of change details to all relevant persons
- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events

3.4. Encryption[18]

3.4.1. Encryption Standard

3.4.1.1. All IGEL encryption shall be done using approved cryptographic modules. Common and recommended ciphers include IBE, FPE, AES 256, Triple DES and RSA. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys

[17] ISO A.12.1.2

[18] ISO A.10

must be of a length that yields equivalent strength. IGEL's key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.[19] All private keys for encryption must be password protected and not stored in the clear on systems.

3.4.1.2. Application of encryption must be used in:

- website channel encryption (SSL)
- Remote access to IGEL Systems (SSH and RDP)
- email encryption (channel and/or content)
- full disk encryption (Employee Laptops)
- secrets management

3.4.1.3. No Proprietary Encryption Algorithms
The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IGEL IT. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

3.4.2. Workstation Laptop and Mobile Device Encryption

3.4.2.1. All devices containing Confidential or Sensitive Data must use an approved method of encryption to protect data at rest.

3.4.2.2. Unless approved by IT and Security, users are expressly forbidden from storing Sensitive Data on mobile devices not issued or supported by IGEL.

3.4.2.3. Laptops must employ full disk encryption with an approved software encryption package

3.4.2.4. All keys used for encryption/decryption must meet complexity requirements in the Password policy.

3.4.3. Encryption Key Management

3.4.3.1. Cryptographic keys must be stored securely in the fewest possible locations and forms.

3.4.3.2. Key generation procedures must produce strong keys.

3.4.3.3. Cryptographic keys must be distributed and stored in a secure manner.

3.4.3.4. Retired keys may not be reused.

3.4.3.5. Management of key parts requires split knowledge and dual control.

3.4.3.6. Access management and Segregation of Duties must be enforced to prevent unauthorized substitution of keys.

[19] Will be implemented in 2020 under new CSO.

3.4.3.7. Access to cryptographic keys must be restricted to the fewest number of custodians as necessary.

3.5. Secure Development

3.5.1. Secure Development Principles

3.5.1.1. Secure Methodologies

IGEL employs secure methodologies during the design and implementation of IGEL products and services. It incorporates best practices in software and operations design and implementation processes with security and vulnerability reviews throughout their lifecycle so that implementation ensures that IGEL products are only used as intended and are not vulnerable to attack or abuse.

3.5.1.2. Standard Secure Development Principles - OWASP and CERT

As a baseline, IGEL uses secure development principles based on the CERT Secure Coding Standards and OWASP Top 10 among other sources.

Secure development principles include but are not limited to: threat modeling, input validation (prevent XSS, injection flaws, malicious file execution, etc.), proper error handling, secure cryptographic storage, secure communications, proper role-based access controls, prevent insecure direct object references, prevent CSRF, secure authentication and session management, prevent insecure cryptographic storage, properly encrypt authenticated and sensitive communications, restrict URL access, peer code review.

3.5.1.3. Feature Vulnerability Reviews

Vulnerability and risk assessments must be completed during feature and user story reviews by engineering, operations, security and product management teams. These assessments include:

- Checklist review of feature against known vulnerabilities and attacks.
- Brainstorming and discussion around possible new risks and attacks based on the context of the features.
- Note and review any existing related products for similar vulnerabilities.
- Documentation and recording of the findings and decisions made to address the findings.

3.5.1.4. Code and Configuration Reviews

During implementation and maintenance, all source code and configuration systems must be reviewed by another team-member before product ship. Code and configuration reviews include:

- Checklist review by team-member of code against known vulnerabilities and attacks.
- Automated code scan by 3rd party source code review systems

3.5.1.5. Software Vulnerability Reviews

Products that have been released require regular review for vulnerabilities and attacks. These reviews shall consist of:

- Internal penetration testing for every new software release
- Annual third-party scans and penetration tests of all current releases

3.5.1.6. Service Vulnerability Reviews

Services that have been released require regular review for vulnerabilities and attacks. These reviews consist of:

- Quarterly internal scans and penetration tests of cloud products and services
- Annual 3rd party scans and penetration tests of services

3.5.1.7. Security Checklists

Engineering must be aware of common software vulnerabilities and must go through this checklist to note whether they are aware of the vulnerability and also whether this product is vulnerable both during design and implementation. All vulnerability checklists are reviewed and updated with all relevant internet vulnerability notifications and announcements (US-CERT, NIST, SANS, etc.) by IGEL engineering and IT. The “Engineering/Ops Aware” checklist is intended to ensure engineering and operations teams have addressed all security issues as specified in the Secure Programming and Operations cookbooks. Enter either “Yes” or “No” as appropriate. The “Product Vulnerable” checklist is a summary of the vulnerabilities (potential or otherwise) of the product under review. Appropriate responses are one of “Yes”, “No”, or “N/A”. Any “Yes” answers must be accompanied by a reference to the corresponding VAMA entry section. “No” and “N/A” entries must provide a synopsis as to why the product is not vulnerable or the vulnerability is not applicable.

3.5.2. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications should:

- support authentication of individual users, not groups
- not store passwords in clear text or in any easily reversible form
- provide for role management such that one user can take over the function of another without knowing the other's password
- support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible

3.5.3. Secure Development Training

- All development and QA engineers shall take secure development training sponsored by IGEL on an annual basis. The training will incorporate the secure methodologies and standard secure development principles used by IGEL.

3.6. Vulnerability Assessment[20]

3.6.1. Security is responsible for identifying significant security vulnerabilities that may affect IGEL assets and for marking recommendations on remediation based on the threat.

3.6.2. Internal production vulnerability scans are conducted on a regular or on-going basis in accordance with applicable compliance requirements.

3.6.3. Security is responsible for monitoring the status of each vulnerability identified, tracking any changes in the status of the vulnerability (e.g. exploit availability, patch availability, etc.), and updating the risk score to reflect these changes.

3.6.4. Patch Implementation

3.6.4.1. The appropriate operating groups are responsible for patching to meet the Priority Ranking.

3.6.4.2. Responsibility for patch quality assurance, patch distribution, and adding patches to standard images/sources is determined by each support group.

3.6.4.3. Implementation is dependent on the Priority Ranking of a patch and may include:

- Automated application of a patch or operational change to a system
- Blocking the system's network access until the patch is applied

3.7. Risk Assessment

3.7.1. Scope

Risk assessments (RA) can be conducted on any entity within IGEL or any outside entity that has signed a Third Party Agreement with IGEL. RAs can be conducted on any information system, to include applications,

[20] ISO A.12.6.1

servers, and networks, and any process or procedure by which these systems are administered and/or maintained. IGEL Engineering performs RAs for all feature and code reviews.

3.7.2. Policy

The execution, development and implementation of remediation programs is the joint responsibility of IGEL IT and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable as well as in the development of a remediation plan.

3.7.3. Risk Assessment Process

- IGEL Engineering performs code and feature vulnerability assessment for every release.
- IGEL Engineering performs security check during code review and build process.
- IGEL Solutions Engineering provides customer feedback
- IGEL Product Management evaluates customer requirements
- IGEL Compliance regularly reviews the internal and third party assessments/feedback, makes improvement recommendations, creates remediation plans as needed, and coordinates implementation to reduce risk and improve the quality with IGEL and IGEL products.

3.8. Information Security Incident Management[21]

Information security incident management is managed by Security according to the IGEL Security Incident Response Plan, which shall be formally documented in 2020.

3.9. Vendor Security[22]

Vendor Security is managed by Security according to the IGEL Vendor Management Policy, which shall be formally documented in 2020. Any external systems that interact with or connect to IGEL systems or that process, store or transmit Sensitive Information shall be subject to the IGEL Vendor Management Policy.

3.10. Disaster Recovery and Business Continuity[23]

IGEL manages DR/BC via the Disaster Recovery Plan and the Business Continuity Plan, both of which are reviewed at least annually and updated as

[21] ISO A.16

[22] ISO A.15, NIST AC-20,

[23] ISO A.17, NIST CP-1

needed. Both of these plans are part of IGEL's Information Security Management System and maintain the same purpose, scope, roles, responsibilities, management commitment, compliance, and departmental coordination as referenced in this Information Security policy unless otherwise noted in those plans. IGEL's current Disaster Recovery Plan and Business Continuity Plan will be finalized and approved in Q2 2020.

4. Information Security Governance

4.1. Information Security Management[24]

The IGEL Information Security Management System (ISMS) is governed by the IGEL ISMS Manual (to be finalized in 2020), certain details of which are outlined in this section.

4.1.1. Security Team

The Security team under the leadership of the Chief Information Security Officer have a key role in achieving IGEL's information security objectives: maintaining the confidentiality, integrity and availability of IGEL's services and protecting Customer Data.

4.1.2. Roles and Responsibilities

4.1.2.1. Executive Committee (CEO and their designees)

Executive Committee provides overall governance, funding, commitment and support for security, ensures IGEL's security goals are aligned with IGEL's business strategy, and promotes the continual improvement of the information security management system.

4.1.2.2. Security Review Committee (SRC)

SRC provides a cross-functional advisory role in ensuring the continual suitability, adequacy and effectiveness of the ISMS. The SRC has cross-functional representation from various organizations functions including: HR, IT, Security, Legal, Engineering and Product.

4.1.2.3. Chief Information Security Officer[25]

4.1.2.3.1. The Chief Information Security Officer is the IGEL authorizing official for the IGEL security program/ISMS and all security compliance certifications.

4.1.2.3.2. The Chief Information Security Officer reviews and authorizes the security program/ISMS prior to commencing operations and has full oversight of the entire program on behalf of the Executive Committee.

[24] ISO A.6.1

[25] NIST CA-6

4.1.2.3.3. The Executive Committee shall review the authorizing official designation at least every three years or as needed.

4.1.2.3.4. The Chief Information Security Officer may designate any responsibilities to Security team full-time staff.

4.1.2.4. Security Team

The Security Team is responsible for setting information security requirements and plans and assuring that security processes are implemented as agreed to by the respective teams as well as:

4.1.2.4.1. Define overall information security scope, strategy and direction.

4.1.2.4.2. Establish and maintain the Information Security Policy.

4.1.2.4.3. Meet security compliance requirements.

4.1.2.4.4. Define and implement a security risk assessment process.

4.1.2.4.5. Plan and coordinate the availability of adequate resources for establishment, implementation, maintenance, and continual improvement of the information security management system.

4.1.2.4.6. Communicate to department managers the importance of effective security management and conforming to security system requirements.

4.1.2.4.7. Ensure the information security management system achieves its intended outcomes.

4.1.2.4.8. Direct and support staff to contribute to the effectiveness of security.

4.1.2.4.9. Promote continual improvement by monitoring and reporting security management system performance.

4.1.2.4.10. Reporting on the continuing suitability, adequacy, and effectiveness of the ISMS to the Executive Committee at least annually.

4.1.2.5. Department Managers

4.1.2.5.1. Manage execution of information security policies in their areas of business.

4.1.2.5.2. Develop appropriate security standards and procedures for their areas of business.

4.1.2.5.3. Training and communicate information security policies and standards to their staff.

4.1.2.5.4. Ensure applicable organizational security objectives are incorporated into departmental projects, budgets and staff priorities.

4.1.2.5.5. Collect and report security metrics to support ISMS evaluation by the Security Team.

4.1.2.6. Asset Owners

4.1.2.6.1. Manage day to day operations of information security controls as it pertains to their assets.

4.1.2.6.2. Assessing and monitoring controls to ensure compliance and report situations of ineffectiveness of controls to Security.

4.1.2.6.3. Maintain updated asset inventory as applicable.

4.1.2.6.4. Manage identity and access authorization for users who have a business need for their information assets.

4.1.2.7. Marketing (Publicly Accessible Information Management)[26]

4.1.2.7.1. The Chief Marketing Officer (CMO) is responsible for managing any information posted about IGEL onto publicly accessible information systems (e.g. IGEL external website, social media accounts, blogs, and press releases).

4.1.2.7.2. The CMO may create a Public Content Policy for publicly accessible information management.

4.1.2.7.3. CMO is authorized to post information regarding IGEL onto publicly accessible information systems.

4.1.2.7.4. CMO is responsible for training staff and contractors to ensure publicly accessible information regarding IGEL does not contain nonpublic information.

4.1.2.7.5. At least quarterly, CMO must review the content of publicly accessible information systems for nonpublic information and remove if necessary.

4.1.2.7.6. CMO may delegate any responsibilities under this section to other IGEL staff.

4.1.2.8. Third Parties

4.1.2.8.1. External Authorities
External authorities such as law enforcement and other designated authorities may be contacted with regards to a security issue or incident if deemed appropriate by Security.

4.1.2.8.2. Information Security Associations
IGEL maintains relationships with various information security related associations and forums as a means to improve knowledge, learn best practices and stay current with the information security industry.

[26] NIST AC-22

4.2. Information Security Policy Management[27]

4.2.1. Ownership

The Chief Information Security Officer oversees the development and maintenance of the information security policies and may designate a governance team to develop, manage, and oversee the review process for these policies

4.2.2. Review

The Information Security Policy is reviewed by the Chief Information Security Officer with input from any applicable stakeholders at least on an annual basis. Any material policy changes will be reported to the applicable stakeholders.

4.2.3. Availability

The Information Security Policy is available to all IGEL employees and contractors via the employee portal. These policies are also available to interested parties at the discretion of the Chief Information Security Officer and designees.

4.3. Legal Review[28]

4.3.1. Identification of Applicable Legislation

All information security policies and standards along with all IGEL privacy policies and standards are periodically presented to IGEL legal counsel for review and revision for compliance with all applicable laws and regulations in the United States as well as any applicable jurisdiction where IGEL processes data, including but not limited to PII. The information security policy so reviewed constitutes the documentation of such applicable governmental laws and regulations. The dissemination of the information security policy and standards constitutes the dissemination of such applicable governmental laws and regulations.

4.3.2. Intellectual Property Rights

Obtaining, distributing or using unlicensed copyrighted software or information without proper authorization from the copyright holder is prohibited. IGEL personnel must respect at all times all copyright protections regarding the use of software and information, and must attribute authorship where appropriate.

4.3.3. Responsibilities

4.3.3.1. IGEL legal counsel is responsible for reviewing information security policies and standards for compliance with applicable governmental laws and regulations and for identifying, defining, documenting and disseminating contractual obligations for information system use.

[27] ISO A.5.1, A.18.2

[28] ISO A.18.1

4.3.3.2. Security, IT and TechOps are responsible for submitting for review, documenting and disseminating information security policy and standards, tracking and managing software and for monitoring and managing systems and network access and use.

5. Security Assessments[29]

5.1. Compliance Assessments Policy and Procedure

5.1.1. IGEL shall undergo and provide full cooperation for any independent third-party security assessments based on executive-committee approved compliance certifications.

5.1.2. The scope of such assessments shall be determined by Compliance in conjunction with Security and be based on the predefined scope of the underlying certification framework.

5.2. Annual Assessments

IGEL shall undergo regular and ongoing assessments that have been approved by the executive committee, will be coordinated through Compliance and have the full cooperation of all relevant IGEL departments.

6. Enforcement[30]

IGEL personnel must abide by all information security policies and standards at all times. Violation of any of the requirements of this policy and applicable standards by any employee will result in suitable disciplinary action, up to and including termination and referral to law enforcement, if applicable.

7. Exceptions

7.1. Exception to Existing Security Policy or Standard

An exception to a published policy or standard may be granted in these circumstances:

- Temporary exception, where compliance would disrupt critical operations
- An alternative solution that is a better fit and provides equivalent security
- A superior solution is available
- A legacy system is being retired
- Lack of resources that prevent compliance with an existing policy

Exceptions will be documented and managed by Security in an exceptions spreadsheet.

[29] NIST CA-1, CA-2

[30] ISO A.7.2.3

7.2. Requesting an Exception

The requestor must open a system of record request (e.g. email it-support@igel.com)with the following information:

- Policy or standard to which you are requesting an exception
- Detailed description of the variation from the Policy/Standard you are requesting. Attach applicable documentation if necessary.
- If exception is temporary, state specific start and end time/dates or the dependent conditions or activities.
- Justification of the exception in as many applicable categories below:
    - Business Need: state how exception will improve performance and/or functionality to IGEL users/customers or how rejecting exception would degrade performance.
    - Risks: define risks to IGEL or Customers that exception mitigates
    - Costs: list costs for improved/maintained performance/functionality
    - Technical: list technical problems the exception resolves and/or introduces

7.3. Review of Exception Request

The Security team must evaluate the exception request under these criteria:

- Deny request if business need does not outweigh security risks, costs, or potential technical problems.
- Record the grant or rejection of the exception in the system of record case.
- Rescind temporary exceptions upon termination date/end of dependent conditions
- Create a task in the system of record case to review the continued applicability of exception at least annually.

8. Control Framework Mapping

Current control framework mapping conducted in line with the policy and corresponding control via footnotes.

9. Document Management and Approval

9.1. Current Approval

Title	Approver	Date
Product Security Manager	Mathias Huber	2020-04-22
Vice President IT Infrastructure	Tim-Oliver Felsen	2020-04-22
Compliance Manager	Jennifer Ortmann	2020-04-22
VP Legal, Compliance and Information Security (North America)	Devanshu Patel	2020-04-22

9.2. Review and Revision History

Information Security Policy is reviewed at least annually and updated when necessary.

Date	Author	Status/Change
2020-04-09	Devanshu Patel	Version 1.0 combined from separate policies.