**IGC Security Policies**

**Adam Hoffmeister**

**Preamble**

Our security policies exist to provide confidentiality, integrity, and availability of our information and resources. Compliance to our security policy is mandatory. Enforcement is handled by the CISO. Ensure you have fully read our procedures and policies and apply them were fit. Failure to comply will result in disciplinary action. The severity of the discipline ranges from a warning, additional training, suspension, or termination. These are further defined by our standards and guidelines.

**Access Control**

IGC operates under a role-based access control model. This limits the harm that can be caused to the organization as only employees have permissions for their job task, and nothing additional. Employees are given a set of roles that allow them the permission to read, write, or execute on that specific task or duty. For example, an accounting employee can see, but is not able to modify the salary for the board of directors. In addition to a passphrase, a two-factor authentication code is required to login to authorized systems. The code is sent via text-message when the user logins.

**Integrity Model**

IGC uses the Clark-Wilson security model to prevent unauthorized users from making modifications and to prevent improper authorized modifications. This maintains our internal and external consistency. Employees may only read and write for what they are granted to. Otherwise, they need explicit trust from a manager to modify outside their permissions. For example, an employee from HR would need a manager to edit the financial records database. The initial permissions are determined by the CISO, while department managers can assist in day-to-day transformation processes.

**Operational Security Model**

Various forms of security layers are deployed at IGC. Multiple firewalls are applied to network interfaces with intrusion detection in place. The firewall and authentication systems have audit logs to keep track of events. Failed authentication attempts will result in the user being locked out. The backups for sensitive HR and customer data are fully encrypted and duplicated off site.

**Least Privilege Policy**

An individual should only have the needed permissions to perform their tasks and no extra privileges should be granted. This is important because it limits possible damage that could affect the organization.

**Security Awareness, Training, and Education Policy**

General awareness training is required for every employee of IGC and is annually scheduled. Additional specialized training is provided to jobs that deal with company security and require certifications. These mandatory educational courses are taught to the following departments: Systems and Networking, Accounting, Customer Support, and Human Resources.

**E-Mail Policy**

The electronic mail service policy provides staff with the allowed use of IGC’s e-mail service. This policy covers incoming and outcoming e-mail to any IGC owned e-mail or device that is capable of such means.

**Monitoring**

Without or without notice, IGC may search for and read the contents of any email (specified above). This may be done to investigate a security issue or to resolve a company issue. Statistical measurements are also taken for historical means and to ensure the systems are working as intended.

**Secure Data Center**

The data center is centrally located in the building on the 3rd floor for network routing. There are water sensors in the case of water piping leaks. It is elevated off the ground to allow for wires to be ran under the servers. Additionally, there is solid ceiling with outlets to route cables upwards. Physical access is restricted by a door with a smart card, no windows are present. The room has a dedicated AC system that has built in alarms in the case of failure. There is a multiple camera system for video surveillance. The servers are all plugged into a UPS which is backed up by our generator system.

**Encryption**

Encrypting for IGC needs to be done using a robust and reliable algorithm. We prefer SHA-256 (or greater) for encrypting and hashing. Any data such as computer passwords, personal data, and financial data needs to be encrypted. Private and symmetric keys need to be securely stored on an offline and unplugged drive. Ensure that your key has a passphrase and is generated using RSA-2048. For file data, 3DES is used to store and send encrypted data.

**Private Key Infrastructure (PKI)**

For most of our PKI needs, we use a Diffie-Hellman solution to exchange keys electronically. This allows our staff to securely authenticate and to encrypt messages between other parties. Senders cannot deny they sent the message as they send it using a private key. For our Active Directory, an in-house solution is used for auto-enrollment which encrypts the workstations to the domain controllers. Web certificates, personal keys, and SSL certificates all need to be generated with 2048 bits minimum. Certificates should be set to a max lifetime of 2 years.

**System Security Configurations**

Only place actively used protocols in the network configuration. No unnecessary services, modems, or shares should be present. The administrator account needs an obscure name and a strong passphrase. All other unnecessary user accounts must be deleted.

Systems need to be configured with an antivirus that handles automatic updates and scans. Every machine needs a firewall between it and the Internet, with an additional software firewall. Systems are automatically patched with our centralized solution.

Floppy disk and CD drives shouldn’t be installed on machines unless needed. Other bootable devices need to be disabled in BIOs, with a password set.

**Security Logs**

Logs are reported to an outside, secure facility. They are replicated and compressed with a password during our backups. When accessed, a report is made logging the individual who accessed and the timestamp. Modifications are completely disallowed.

**Network Security Design**

Network access control is used to ensure systems have anti-virus, patches, and a firewall. Employees are only permitted to connect authorized devices to the network. No routers, modems, access points, or similar are permitted. WPA2 is used for our wireless encryption.

The wiring closet has a secured cabinet, along with smart card door. No unauthorized employees are permitted to interact with the equipment.

Our firewall drops the following: ICMP Echo requests, UDP packet with DF bit, and ICMP redirects from not the router. We use load balancing to prevent SYN floods. The timeouts on ACK responses and SYN cookies is minimized. Our DNS needs to remain constantly patched.

Switches are operated on the network layer. The number of MAC addresses should be limited per port. Also, DHCP guarding should be used to stop other DHCP traffic.

For our intrusion detection system, we use a host-based system with signature-based detection. Outside connections need be tunneled to access internal services. Phone data and connections are handled over VoIP.

**Secure Programming Environment**

To ensure security, we follow a specific development model. The process is: requirements, system architecture, coding, and testing. It is important to have security as an imbedded step in the processes. If there are any specific security requirements, that should be brought up first. The architecture needs to be chosen with security in mind, following the requirements. Coding needs to be done with peer reviews. Testing needs to readdress the requirements and ensure they were met. It also needs to address any unexpected behavior which could cause a security issue.

**Code Review**

Before any code is deployed, it must be peer reviewed. Any application working with financial, employee, or customer data needs to have a formal code review and inspection. Other work requires a team review, regardless of the application. For quick patches or bug fixes, the code can be passed around to get it deployed quickly. After feedback and corrections have been made, we expect a follow-up review. This verifies that the code has been corrected and there are no new defects.

**Business Continuity Plan**

We have redundant server hardware ready in case of a disaster. In addition, we have images for each server and machine. This allows us to restore them quickly. The full backups, which are already maintained on and off site, can be restored at any time. We automatically take differential backups every 24 hours and old copies are archived for 2 weeks. Our dedicated system administrator is the main contact for systems that process critical data. In the case of critical failure, the admin leads the response team which consists of the IT department, a member of legal, and public relations.

The whole building has backup power in case of an outage. There is a generator capable of producing power for 24 hours. In the case of a network outage, we have an additional line from another utility provider. The third backup plan for network is to engage our mobile data service provider.

In the case of major downtime past 12 hours, we will engage our alternative site. This is the present area where we keep offsite logs and backups. Moving our servers there would be a last resort.

Every month we test the procedure and backup/restoration methods, along with the generator. This ensures the process can be done fluently and quickly.

**Forensics and Investigation**

The Computer Incident Response Team (CIRT) is made up of the IT department, a member of legal, and public relations. All these employees are specifically trained for incident response. In the case of an issue, we first examine logs and report the situation. If anything is amiss, we immediately will contact our forensics team. They assist with investigating and analyzing the systems for intruders, policy violations, and other attacks. The team needs to be able to respond within 1 hour of the incident. Our CIRT team can handle any critical issues until then.

**Signature Sheet**

Our policies:

* Acceptable Use
* Disposal and Destruction
* Due Care
* E-Mail Monitoring
* E-Mail Usage Policy
* Employee Hiring and Promotions
* Employee Retirement, Separation, or Termination
* Internet Usage Policy
* Need to Know
* Password Management
* Privacy Policy
* Records Retention
* Separation of Duties
* Service Level Agreements

By signing you state that you have read and understood the policies.