**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.

**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.