**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.

**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.

**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.