**IGC Security Program: The Beginning**

**Adam Hoffmeister**

**Who is responsible for overall creation/enforcement of it?**

The technology directory CIO is responsible for the creating and enforcing the security policy. They are chosen because they know how the infrastructure and services are setup, so they know the best ways to secure them. Plus, as they are responsible for breaches, they will want the best security and policies in place. In most cases, a CISO will be appointed to maintain the program instead of the CIO.

**Where does it originate from (what body? CEO, Board, etc.)?**

The security policy originates from the board of directors. This allows for the board to agree on changes for the program’s roles and policy changes.

**How does it support the business?**

Security policies bring CIA to the business: confidentiality, integrity, and availability. These three ensure that only authorized individuals can view information, edit/delete information, and that the data is always there when required.

**What is the governance for the security program document?**

The security program needs support from the highest roles in order to succeed. It starts from the board of directors where they allow the CEO to establish the program and appoint the CIO to manage it. From there, the CIO creates the department and appoints a CISO. The department is then lead by the CISO to create the program, hire additional staff, and maintain it. The CISO then has responsibility for the overall program.

**Create a preamble page which includes conditions for violating policies.**

Compliance to our security policy is mandatory. 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.

**Create an initial policy page with list of desired 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