IBM Security Business Unit (BU)

IT Security Implementation Guidelines (SIG)

Owner – Dimple Ahluwalia

Document Version: 0.1

Document Control Number: ISS-SECBU-XXXX

Total Pages: Y

1. Table of Contents

[1. Table of Contents 2](#_Toc521502744)

[2. Document Control 3](#_Toc521502745)

[1. Organization 4](#_Toc521502746)

[1.1. Scope and Applicability 4](#_Toc521502747)

**[1.1.1](#_Toc521502748)****[General Guidelines](#_Toc521502748)** [4](#_Toc521502748)

**[1.1.2](#_Toc521502749)****[Scope and Applicability](#_Toc521502749)** [6](#_Toc521502749)

**[1.1.3](#_Toc521502750)****[Scope Exclusion](#_Toc521502750)** [7](#_Toc521502750)

[1.2. Compliance 8](#_Toc521502751)

1. Document Control

|  |  |
| --- | --- |
| * + - * 1. **Document Name** | * + - * 1. Security BU IT Security Implementation Guidelines ( SIG) |
| * + - * 1. **Document Control Number** | * + - * 1. ISS-SECBU-XXXX |
| * + - * 1. **Document Identification** | * + - * 1. Version Draft 0.1 |
| **Owner / Approver Identification** | * + - * 1. Dimple Ahluwalia         2. Business Information Security Officer (BISO), Security Business Unit |
| * + - * 1. **Author** | * + - * 1. Neetee Pawa |
| * + - * 1. **Document Reviewer(s)** | * + - * 1. The following personnel will review the initial documentation and subsequent changes:   Dimple Ahluwalia – Security Business Unit Information Security Officer (BISO)  Elizabeth Dunphy – Deputy CISO, IBM Security |
| * + - * 1. **Review Plan** | * + - * 1. This document should be reviewed by all parties on a annual basis and when need arises. * Next Review is: **10/10/19 or as needed before then** |
| * + - * 1. **Latest Level** | * + - * 1. This document resides within the QMX document repository |
| * + - * 1. **Distribution** | * + - * 1. Copies of this document may be obsolete. It is the users’ obligation to verify they are using the most current edition. This document should be removed from use when obsolete. |

| **Revision History** | | |
| --- | --- | --- |
| **Date** | **Revised by** | **Changes** |
| **19-July-2018** | **Neetee Pawa** | Created |
|  |  |  |

1. Organization

This document establishes the IT Security requirements for the protection of IBM Security Business Unit (SBU) and the information assets the business unit owns. This policy has been developed to provide guidelines for implementing and maintaining security best practices around securing Information assets. The IBM Security BU Security Implementation Guide (SIG) is designed to complement the [IBM IT Security Standard (ITSS).](https://pages.github.ibm.com/it-standards/main/) Remember that the goal is to identify and apply appropriate security controls to systems based on the risk to IBM, not to facilitate "checklist" compliance.

* 1. Scope and Applicability

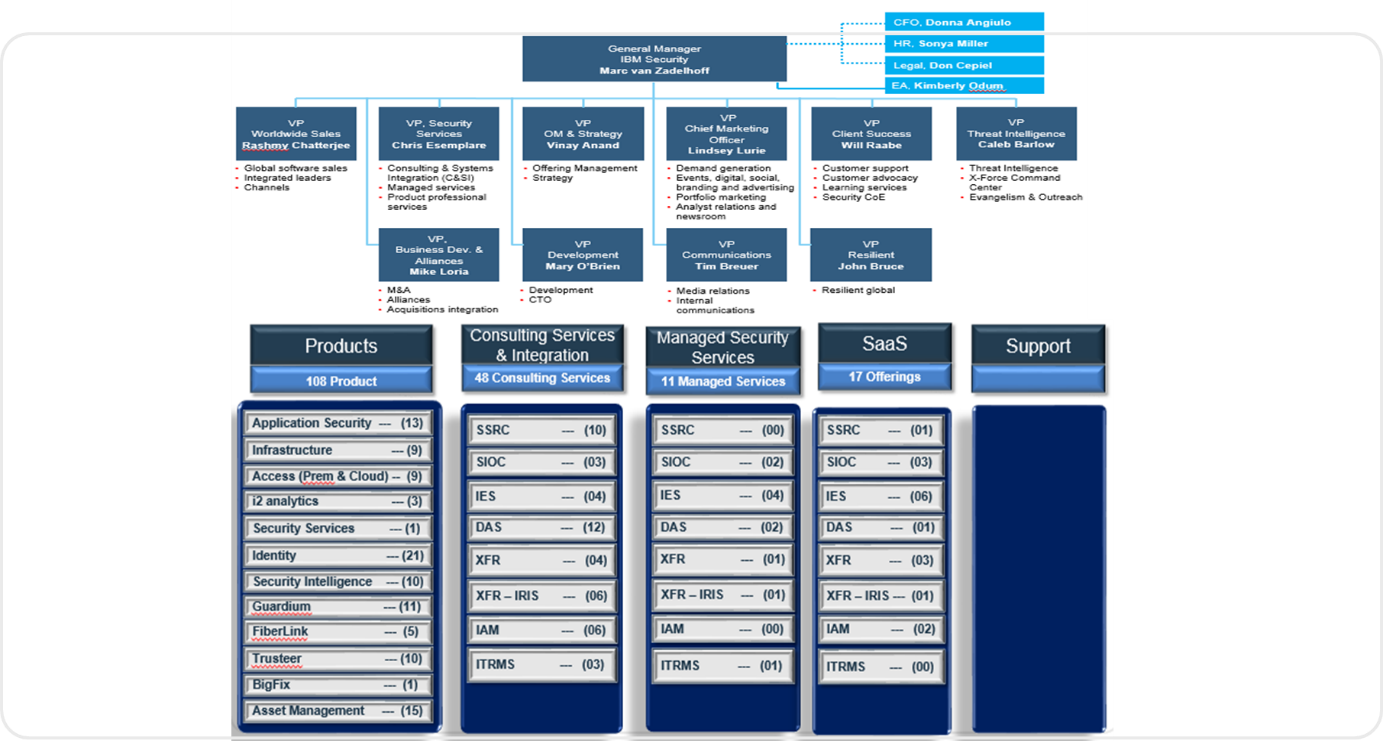
|  |
| --- |
| Related ITSS Requirement |
| *This standard establishes the principles and requirements for the protection of IBM world-wide information technology systems and the information they contain. The principles and requirements in this standard are defined by the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO). The standard applies to all IBM operating units, corporate staffs and subsidiaries, without exceptions.*  *IT assets, including infrastructure, that are dedicated only to a single IBM customer, are outside the scope of this standard and are instead governed by requirements established by contract with the customer.* |

### **General Guidelines**

This section provides general guidelines for the understanding and implementation of the Policy Statements:

1. The policy outlines the minimum baseline requirements for information security to be followed and implemented in scope SBU operating units.
2. In order to comply with the requirements specified in the policy, the individual SBU locations may choose to implement custom processes and procedures to suit the business and compliance requirements, IT environment resulting in processes/ procedures specific to individual operating unit.
3. If the customer, regulatory, legal or security compliance requirements of a specific SBU location has a conflict or has higher degree of requirements than the requirements under this Policy, then the specific requirements will supersede these Policy Statements (e.g. US Federal Financial Institutions Examination Council – FFIEC or General Data Protection Regulation - GDPR). Where the discrepancy creates a lower level of security then a deviation must be raised with the Business Unit Information Security Officer (BISO)
4. The Policy Statements are mandatory requirements and factored in to any technical or operational requirements. To indicate additional controls that are applicable, certain clauses of the Policy Statements are phrased to include ‘as/wherever applicable’ or ‘as per technical feasibility’. SBU users are recommended to consider such controls through business/technical feasibility analysis for their in-scope systems.
5. This Policy is applicable to all users of the systems covered under the Scope of this Policy. Where appropriate distinction may be made for privileged (e.g. root / administrator) and non-privileged users or all users. The Policy can be referred to and enforced by the respective IT Security and Compliance Teams.
6. The ‘Associated Processes and Guidelines’ Section of the Policy enlists the recommended processes which may be documented to assist in the implementation of the Policy.
7. The ‘Roles and Responsibilities’ Section provides only indicative list of roles and responsibilities. The specific assignment of the role or responsibility may vary depending on the Operating team's organization structure.

### **Scope and Applicability**

SIG is applicable to the following Security BU operating units for IT elements covered hereafter. 

The scope of SIG policy implementation has been categorized into three major areas as narrated below:

* Systems Scope
* Process Scope
* Location Scope
* **System Scope -** The following systems supporting seamless operations of SBU business are included in the scope. ISG will address high level security requirements for the following systems:
* Network devices (routers, firewalls, switches, IDS / IPS etc.)
* Business Applications
* Servers
* Databases
* Middleware
* Operating systems
* Emerging technologies such as mobile and collaborative platforms
* Cloud computing Environment.
* Virtual Machines
* Containers
* **Process Scope** - IT processes enabling the business automation facilitated by IT Infrastructure. The major IT processes within scope are:
* *Network Management* – includes processes for operation, administration, maintenance and provisioning of the network components.
* *Server Management* – includes processes for configuring, managing and administering the components within the servers.
* *Database Management* – includes processes for creating and managing databases.
* *Application Management* – includes processes for managing the operation, maintenance, versioning and upgrading of an application throughout its lifecycle.
* **Location Scope** – SIG policy will be applicable for all IBM Security Computing Environments, Labs, Data centers and locations supporting IBM Security BU’s business operations.
  + Production servers (virtual or physical servers),
  + Staging Servers
  + Test Servers
  + Development Servers
  + Service Offering.
  + QA Servers

### **Scope Exclusion**

This policy does not apply in the following situations

1. IT assets, including infrastructure, that are dedicated to a single IBM Client, are outside the scope of SIG and are instead governed by requirements established by contract with the Client. If the contract does not explicitly include security requirements or reference to the governing IT security policy then the requirements of this document shall be used instead.
2. IT assets, including infrastructure, that are deployed within a Client environment are outside the scope of SIG and are instead governed by requirements established by contract with the Client. If the contract does not explicitly include security requirements or reference to the governing IT security policy then the requirements of this document shall be used instead.
3. MSS managed devices
   1. Compliance

This standard is in effect immediately upon publication. Compliance with this standard is mandatory, and operating units are responsible for complying by 15 February 2019. Compliance with the control requirements within this document are mandatory and subject to Audit inspection. Systemic deviations or alternative requirements can be brought forward by the [Business Information Security Officer](https://w3-connections.ibm.com/wikis/home?lang=en-us#%21/wiki/W0d34e3ec2088_4562_8496_752f0342bb4b/page/Who%20are%20the%20BISOs) (BISO). Deviations from these compliance criteria is documented and approved in accordance with [Security BU](https://w3-03.ibm.com/ibm/documents/corpdocweb.nsf/ContentDocsByTitle/Corporate+Instruction+FIN+166" \t "blank) Risk Exception Process.