End User Computing Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | Approved by: |
| 1.0 | 10/05/2019 | David H | Initial document |  |
| 1.1 | 30/09/2022 | David H | Added version history |  |
| 1.2 | 22/08/2024 | David H | Reviewed updated sensitivity label unrestricted in line with policy. |  |

**Document Owner IT**

Contents

[Introduction 2](#_Toc8634372)

[Scope 2](#_Toc8634373)

[Risk Assessment 2](#_Toc8634374)

[Controls 2](#_Toc8634375)

[Low Risk EUCs 3](#_Toc8634376)

[Medium or High Risk EUCs 3](#_Toc8634377)

[High Risk EUCs 3](#_Toc8634378)

# Introduction

The expected outcome of this document is to provide an understanding of the End User Computing process and the controls that should be put in place, across the business where End-User computing is utilised.

This policy is referred to as the End-User Computing Policy and is accompanied by the supporting document “End-User Computing Guidelines”

The purpose of this document is to ensure that uses of End User computing are:

1. Appropriate
2. Properly controlled to ensure confidentiality Integrity and availability of all data contained within.

# Scope

This policy applies to End-User Computing (“EUC”), defined as any automated function or program that is managed (developed and/or maintained/supported) within a company business unit.

Existing and potential EUC must be assessed to determine appropriateness for end-user development, using the criteria set out in the “End-user computing guidelines”

EUC are assessed and classified into Low, Medium, or High risk, depending on the outcome of the risk assessment. The higher the risk the stronger the controls to ensure their integrity of functions are maintained.

# Risk Assessment

Each End-user computing must have an adequate of controls applied to it based on an assessment to determine the level of risk that EUC creates. The level of risk should take the following into consideration:

* If the EUC support financial reporting and/OR
* Supports Risk Reporting and/OR
* Supports Key operation processes and/OR
* Records or maintains personal information (PII, SPII)

For further details please review the “End-User Computing Guidelines”

# Controls

All departments utilizing EUCs shall identify an individual accountable for managing these EUCs. This management accountability includes:

* Ensuring that all EUCs fall within the criteria for end-user development;
* Ensuring that risk assessments are performed to identify appropriate level of controls required for each EUC;
* Maintaining a current inventory of medium and high risk EUCs;
* performing an annual inventory review;
* Ensuring EUCs are supported appropriately based on their risk assessment;
* Ensuring execution of required controls based on assessed risk rating;

Low Risk EUCs:

Reasonability checks should be applied to EUC results.

Further EUC controls identified in this document are not required.

Appropriate controls may be identified at management discretion.

Medium or High Risk EUCs:

The following controls are required for all EUCs assessed as medium or high risk:

1. Documentation – sufficient documentation to ensure that the EUC can be used supported and maintained in the absence of the developer and/or primary user.
2. Testing – testing and logic inspection by an individual independent of the development of the EUC, to ensure accuracy and integrity of the functions being performed.
3. Input control – procedures that can be used to protect the integrity of data.
4. Version control – file naming and storage conventions to ensure the most current EUC version is used and past versions can be referenced if required.
5. Access control – documentation of access rights established for users of the EUC and a process for managing access rights, to protect EUCs from unauthorized use.
6. Backup and archive – a process to backup the EUC on a regular basis to ensure availability of the information. (see guidelines for more details)

High Risk EUCs:

In addition, the following controls are required for EUCs assessed as high risk:

1. Change management – a process for logging, testing and approving changes to the EUC prior to use to ensure the EUC continues to meet the intended purpose.
2. Enhanced testing – testing procedures commensurate with level of risk.
3. Enhanced input control – input control procedures commensurate with level of risk.

For details see “End-User Computing Guidelines”.

1. Ownership and Maintenance

This Policy is scheduled for review and revision every two years or at such other times as deemed appropriate or necessary. The Chief Information Officer is responsible for ensuring this Policy’s appropriateness through reviews and revisions, with support from the Legal, Compliance and Internal Audit departments.

# Approval

|  |  |
| --- | --- |
| Name: | [Enter Name here] |
| Position: | [Enter Position Here] |
| Date: | [Enter Date of signing here] |
| Signature: | [Add Signature image here] |