END-USER COMPUTING POLICY
IT-P-009
Date: 10th July, 2014
Stamford International University
End-User Computing Policy

Purpose

The purpose of this policy is to establish control guidelines for key end-user computing (EUC) tools at Stamford International University ("STIU" or "Stamford"). The intent is to define a series of guidelines and procedures to deal with the security and use of EUC tools such as spreadsheets, databases, report writers, etc. This policy is to be used in conjunction with other applicable policies and practices.

Scope

This policy applies to all employees of STIU in all locations including the temporary employees, part-time and contractors, who use Electronic Tools that are:

- Developed and managed by users and process owners, typically within office automation software like spreadsheets, databases, and report tools (e.g. Crystal Reports);
- Not subject to IT general controls; and
- Either:
  - Used to assist with the calculation of an amount that is recorded in the general ledger or as the basis for disclosure in the financial statements (which has a significant financial impact), or
  - Used in the execution of a control that is relied upon by management to support their assessment of the effectiveness of internal controls over financial reporting (e.g., a spreadsheet used to prepare and review reconciliation).

Policy Information

Responsible Office: Department of Information Technology, Stamford International University
Issued Date: July, 2014
# Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Document Number</th>
<th>Description</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>IT-P-009</td>
<td>New Release</td>
<td>10th July, 2014</td>
</tr>
</tbody>
</table>


Contents
Stamford International University ................................................................. 2
End-User Computing Policy ........................................................................ 2
Purpose ........................................................................................................ 2
Scope .......................................................................................................... 2
Policy Information ..................................................................................... 2
Revision History ......................................................................................... 3
Recommendation and Approvals ................................................................. 5
Policy .......................................................................................................... 6
Procedures ................................................................................................ 7
Inventory EUC Tools .................................................................................. 7
Evaluate Risk related to each EUC Tool ....................................................... 7
Determine the Necessary Level of Control ............................................... 8
  High-Risk End-User Computing Tool Controls ....................................... 8
  Medium-Risk End-User Computing Tool Controls .................................. 9
  Low-Risk End-User Computing Tool Controls ....................................... 10
Responsibilities ........................................................................................ 10
APPENDIX A - RISK-RANKING EVALUATION MATRIX ................................ 11
APPENDIX B - OWNER CONTROL CHECKLIST ..........................................12
Recommendation and Approvals

Prepared by:

__________________________
Name: Chavanath Chatchaiyan  
Position: Technology Services Manager  
Date: 10th July, 2014

Approved by:

__________________________
Name: Sourjya Sankar Sen  
Position: Director, Information Technology  
Date: 10th July, 2014

__________________________
Name: Gilles Mahe  
Position: CEO, Stamford International University  
Date: 10th July, 2014

__________________________
Name: Dr. Boonmark Sirinaovakul  
Position: President, Stamford International University  
Date: 10th July, 2014
Stamford International University relies on key EUC tools in the financial reporting process. Given the importance related to the integrity and reliability of the information generated by EUC tools, appropriate measures for ensuring that appropriate controls exist for EUC tools must be adopted.

DEFINITIONS:

- **Access Control** – Limiting access at the file level to EUC tools on a central server and assigning appropriate rights.
- **Archiving** – Maintaining historical files no longer available for update in a segregated drive and locking them as *read only*.
- **Backups** – Implementing a process to backup EUC tools on a regular basis so that complete and accurate information is available for financial reporting and can be restored if the original file is compromised.
- **Input Control** – Ensuring that reconciliations occur to make sure that the data is inputted completely and accurately. Data may be inputted into EUC tools manually or systematically through downloads.
- **Logic Inspection** – Inspecting the logic in critical EUC tools by the Owner each time the EUC tool is used or completed for financial purposes.
- **Overall Analytics** – Implement analytics as a detective control to find errors in EUC tools used for calculations. However, analytics alone are not a sufficient control to completely address risk of financial amounts generated in EUC tools.
- **Version Control** – Ensuring only current and approved version of EUC tools are being used by creating naming conventions and directory structures.
Procedures

Stamford has implemented three high-level steps for ensuring that successful EUC tool controls exist for compliance purposes:

Inventory EUC Tools
All EUC tools used within Stamford International University to support significant financial processes must be inventoried. Further, Stamford must identify how the EUC tools support all significant accounts and financial statement disclosures and their relationship to relevant financial statement assertions. All departments utilizing EUC tools should complete this inventory, including but not limited to, financial reporting, cost accounting, tax, and operations. The Department Head or designee in respective departments shall maintain the EUC tool inventory. For new EUC tools, inventory evaluation must be obtained in the first month that the EUC tool is used for financial purposes. Quarterly, the Dept. Head or designee should re-evaluate all inventoried EUC tools to confirm the risk ranking.

Evaluate Risk related to each EUC Tool
Each EUC tool will be categorized for various risk factors. Risk factors are weighted based on the criticality associated with each risk type. For the following section, the rating scale will be 1 = Low, 2 = Medium, and 3 = High.

Each EUC tool will be evaluated for complexity. EUC tool complexity will be categorized as one of the following:

- **Low** – EUC tools that serve as an electronic logging and information tracking system.
- **Moderate** – EUC tools that perform simple calculations such as using formulas to total certain fields or calculate new values by multiplying two cells. These EUC tools can be used as a means to translate or reformat information, often for analytical review and analysis, for recording journal entries, or making a financial statement disclosure.
- **High** – EUC tools that support complex calculations, valuations, and modeling. These EUC tools are typically characterized by the use of macros and multiple supporting tools where cell values and individual tools are linked. These EUC tools might be considered applications in their own right. They often are used to determine transaction amounts or as the basis for journal entries into the general ledger or financial statement disclosure.

A risk-rating evaluation matrix can be found in Appendix A of this policy. Based on the results of the evaluation exercise, each EUC tool is assigned a risk score and a risk rating. The risk score of each EUC Tool will be based on the complexity evaluation.
The risk score then results in a risk rating:

- 1 to 1.66 = LOW
- 1.67 to 2.33 = MED
- 2.34 to 3 = HIGH

**Determine the Necessary Level of Control**

The risk rating will determine the appropriate combination of controls required to help mitigate the risks inherent in an EUC environment. The following table reflects the mitigating controls required for each risk rating:

<table>
<thead>
<tr>
<th>Control Type</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security / Access Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Input Control</td>
<td>✓</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Backups / Archive</td>
<td>✓</td>
<td>✓</td>
<td>None</td>
</tr>
<tr>
<td>Logic Inspection / Version Control</td>
<td>✓</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Analytics</td>
<td>✓</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

**High-Risk End-User Computing Tool Controls**

The following types of controls will be required for all HIGH-risk EUC tools in order to confirm the reliability of the information contained within the EUC tool:

- **Security & Access Control** – Access to a HIGH-risk EUC tool will be limited to only those employees identified as someone who can create and / or modify a HIGH-risk EUC tool.
  - EUC tool owners (OWNER) and authorized users (USER) are approved by the Controller or designee. Approval must be obtained in the first month that the EUC tool meets the definition of an EUC tool, which is included in the Purpose section of this policy. This approval should be documented and maintained.
  - Both OWNER and USER will have access to the secure network location where the file will reside for modification. Access to this location is limited to appropriate personnel in each area.
  - Access rights for each key network location noted above are reviewed quarterly by the Controller, or designee, to verify that all active accounts belong to active employees and that the access is accurately assigned.
  - HIGH-risk EUC tools must utilize software features, such as cell-locking and password protecting in Excel and locking tables to create read-only access in Access, to protect EUC tool logic.
END-USER COMPUTING POLICY

• **Input Control** – Inspection of inputs MUST be performed each time the HIGH-risk EUC tool is used / completed for financial purposes. A checklist has been developed that contains an item for the OWNER to review all inputs (please see Appendix B).

• **Backups / Archiving** – All HIGH-risk EUC tools MUST be located in a secure network location that is backed up on a daily basis by the Information Technology organization. EUC tools to be retained for historical support will be retained in a folder which will have read only access.

• **Logic Inspection** – Inspection of logic MUST be performed when reviewing HIGH-risk EUC tool modifications.
  - OWNER is responsible for ensuring logic is free of errors that may invalidate the figures within an EUC tool. This is included in the Owner Control Checklist displayed in Appendix B.
  - A change control document is required for all HIGH-risk EUC tools to log changes in formulas and logic (e.g., formulas in Excel, structure in Access, or formatting in Crystal Reports). This would not include data entry changes. For an Excel spreadsheet, this can be accomplished by logging the changes in a separate tab within the workbook. For other EUC tools, a Word document will be sufficient.
  - Formula and logic changes will be independently inspected and approved prior to using the EUC tool for its intended purpose. This is included in the Owner Control Checklist displayed in Appendix B.

• **Overall Analytics** – A reasonableness test must be performed on the EUC tool results and documented. This may include comparison of results to historical amounts or some other external comparative amounts or ratios. This is also included on the Owner Control Checklist displayed in Appendix B.

**Medium-Risk End-User Computing Tool Controls**

The following types of EUC tool controls will be utilized for all MEDIUM-risk EUC tools in order to confirm the reliability of the information contained within the EUC tools:

• **Security & Access Control** – Access to a MEDIUM-risk EUC tool will be limited to the EUC tool owner and any personnel who directly report to the EUC tool owner unless specifically authorized by the owner.
  - Both OWNER and USER will have access to the secure network location where the file will reside for modification. Access to this location is limited to appropriate personnel in each area.
  - Access rights for each key network location noted above are reviewed quarterly by the Controller, or designee, to verify that all active accounts belong to active employees and that the access is accurately assigned.
  - MEDIUM-risk EUC tools must utilize software features, such as cell-locking and password protecting in Excel and locking tables to create read-only access in Access, to protect EUC tool logic.
Backups - All MEDIUM-risk EUC tools MUST be stored in a secure network location. Files stored in a secure network location are backed-up on a daily basis by the Information Technology organization.

Low-Risk End-User Computing Tool Controls

The following types of EUC tool controls will be utilized for all LOW-risk EUC tools in order to confirm the reliability of the information contained within the EUC tools:

- **Security & Access Control** – Access to a LOW-risk EUC tool will be limited to the EUC tool owner and any personnel who directly report to the EUC tool owner unless specifically authorized by the owner.
  - Both OWNER and USER will have access to the secure network location where the file will reside for modification. Access to this location is limited to appropriate personnel in each area.
  - Access rights for each key network location noted above are reviewed quarterly by the Controller, or designee, to verify that all active accounts belong to active employees and that the access is accurately assigned.

Responsibilities

The maintenance of this policy document is the responsibility of the IT Department along with procurement & maintenance of the infrastructure required to mitigate the risks of an EUC environment.

Execution & governance of the procedures documented here are the responsibility of all departments that have an impact on financial reporting.
# APPENDIX A - RISK-RANKING EVALUATION MATRIX

<table>
<thead>
<tr>
<th>Risk Rating:</th>
<th>Low (1)</th>
<th>Medium (2)</th>
<th>High (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>Logging and Tracking</td>
<td>Simple calculations: Totaling</td>
<td>Complex calculations: Macros</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B - OWNER CONTROL CHECKLIST

This checklist is to be completed by the OWNER each time a HIGH-risk EUC tool is used/ completed for financial purposes. Please send all completed copies to the Controller or designee.

Owner: __________________________________________
Spreadsheet File Name: ________________________________
Purpose: __________________________________________

<table>
<thead>
<tr>
<th>OWNER CONTROL CHECKLIST</th>
<th>Y / N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have all inputs been verified?</td>
<td></td>
</tr>
<tr>
<td>Has the EUC tool logic been inspected?</td>
<td></td>
</tr>
<tr>
<td>Is the EUC tool filed in the proper folder?</td>
<td></td>
</tr>
<tr>
<td>If applicable, are all links working as intended?</td>
<td></td>
</tr>
<tr>
<td>Do analytics support the final results?</td>
<td></td>
</tr>
<tr>
<td>For formula and logic changes, has the EUC tool been independently inspected and approved?</td>
<td></td>
</tr>
</tbody>
</table>

___________________    ____________
Signature, Owner                  Date

___________________    ____________
Signature, Independent Approver  Date