I. Purpose:

To provide an enterprise-wide standard, with assigned roles and responsibilities, for conducting an Information System Business Impact Analysis (BIA) in order to assess the potential impact that a loss of IT service(s), or access to information systems and data might have on business operations. The BIA results are used to:

A. Establish operational and information system recovery priorities, and

B. Develop and implement appropriate operational and IT contingency plans to mitigate the potential impact

II. Process:

A. **Information System Classification and Recovery Requirements**: Information System Application Owners shall meet with the Business Operations’ leaders responsible for the operational areas where the information system is used to conduct the BIA and document the results. VUMC Enterprise Cybersecurity Business Resilience Services (VEC BRS) maintains an Information System Business Impact Analysis Template for conducting the BIA.

1. **Business Operation Shall**:

   a. Identify business activities that will be impacted in the event of an information system disruption

   b. Assess maximum tolerable downtime for each core function supported by the information system to determine the Information System Recovery Time Objective (RTO).

      Considerations include but are not limited to:

      i. How long business operations can continue to function using downtime procedures before critical functions can no longer be supported;

      ii. Required staffing levels, staff availability, and staff rotation;
iii. The time it would take to enter or re-enter data into the system once the system is recovered, before the system can be considered operational.

iv. Regulatory or contractual requirements and penalties (including 3rd party entities or organizations with whom VUMC has a business relationship or contractual obligation)

v. Loss of, or delayed revenue;

c. Assess maximum amount of tolerable data loss for each core function to determine the Information System Recovery Point Objective (RPO). Factors to consider include but are not limited to:

i. The amount of data that would need to be entered into the system once the system is made available, and the time it would take to enter this data;

ii. The ability to recover data from other sources (e.g. upstream systems), and the time it might take to organize and backload this data;

iii. Regulatory or contractual requirements and penalties (including 3rd party entities or organizations with whom VUMC has a business relationship or contractual obligation)

d. Classify the type of data being processed or accessed

i. Does the information system use confidential information that may require special handling protocols (due to VUMC operational, regulatory/compliance, and/or business agreement requirements?)

e. Determine the number of end users and end user building locations

f. Determine how the system is accessed

i. Authentication methodology

ii. Access methodology

B. Documented BIA Review and Sign-Off:

1. Once business operations’ leaders have conducted their assessment and completed the BIA template, the Information System Application Owners shall provide a copy of the completed BIA to VEC BRS for review and recommendations.
2. VEC BRS shall review the completed BIA and document their review findings and contingency planning recommendations in the BIA.

3. VEC BRS shall then provide the Information System Application Owners with a copy of the updated BIA for final signatures.

4. Information System Application Owners shall then obtain and document final BIA sign off from operational leadership to indicate:
   a. Agreement with, and approval of, business operations’ Recovery Requirements analysis
   b. Acknowledgement of VUMC Enterprise Cyber Security (Business Resilience) contingency planning recommendations
   c. Business operations can provide their sign-off via an email or formal signature on the BIA

5. Once operational final sign-off has been received, Information System Application Owners shall then provide a copy of the finalized BIA to the appropriate IT infrastructure Owner leader for sign-off. Sign off will indicate:
   a. Receipt and acknowledgement of business operations’ information system recovery requirements
   b. Acknowledgement of VUMC Enterprise Cyber Security (Business Resilience) contingency planning recommendations

6. Once all sign-offs have been received and documented, The Application System Owner shall provide VEC Business Resilience with a copy of the finalized BIA, while maintaining a copy for their own use.

7. VEC BRS Resilience will store a copy of the finalized BIA in a central repository, for record keeping purposes.

C. **Triggers for BIA Review**

1. The BIA is reviewed, at a minimum, on an annual basis, to ensure business operations’ requirements for information system recovery, and information system recovery capability, is aligned with operational objectives. Additional events that may trigger a review include, but are not limited to:
   a. Organizational changes (e.g. change in leadership)
   b. Change in operational priorities
   c. Change in business process(es)
   d. An IT incident that indicates a review is warranted due to misaligned priorities
D. **BIA Responsibility Matrix**

**Responsible** - Person who completes a particular process or step, or leads the people who do; person working on the activity and responsible for implementation.

**Accountable** - Person who is held accountable by top management for implementation; only 1 x “A” per function.

**Consulted** - Person whose advice is sought before a final decision is made and/or implementation takes place; two way communication.

**Informed** - Person or persons who are notified once a final decision has been made or after implementation takes place; position that needs to know of a decision; one way communication.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Business Operations</th>
<th>Information System Application Owner</th>
<th>IT Infrastructure Owner</th>
<th>VEC BRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) Identify business activities that will be impacted in the event of an information system disruption</td>
<td>A, R</td>
<td>R, C</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>c) Assess the impact over time of not performing these activities</td>
<td>A, R</td>
<td>R, C</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>d) Set prioritized timeframes for resuming these activities at a specified level of functionality, taking into consideration the time within which the impacts of not resuming them would become unacceptable</td>
<td>A, R</td>
<td>R, C</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>e) Identify dependencies and supporting resources for these activities, including other information systems, suppliers, outsource partners and other relevant interested parties</td>
<td>A, R</td>
<td>R, C</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>f) Compile results in BIA Template)</td>
<td>C</td>
<td>A, R</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>g) Contribute Information System Contingency</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>R</td>
</tr>
</tbody>
</table>
**Responsible** - Person who completes a particular process or step, or leads the people who do; person working on the activity and responsible for implementation.

**Accountable** - Person who is held accountable by top management for implementation; only 1 x “A” per function.

**Consulted** - Person whose advice is sought before a final decision is made and/or implementation takes place; two way communication.

**Informed** - Person or persons who are notified once a final decision has been made or after implementation takes place; position that needs to know of a decision; one way communication.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Business Operations</th>
<th>Information System Application Owner</th>
<th>IT infrastructure Owner</th>
<th>VEC BRS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning Recommendations, based on Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h) Set next scheduled review date</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>A, R</td>
</tr>
<tr>
<td>i) Provide BIA Sign-Off</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>j) Provide VEC Business Resilience with copy of Final BIA</td>
<td></td>
<td>A, R</td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>k) Store Report in central repository</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>A, R</td>
</tr>
<tr>
<td>l) Monitor for changes in business environment that may trigger BIA review</td>
<td>A, R</td>
<td>C</td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>m) Monitor for changes in IT environment that may trigger BIA review</td>
<td>C</td>
<td>A, R</td>
<td>R, C</td>
<td>I</td>
</tr>
</tbody>
</table>

I. **Lead Author and Content Experts:**

Lead Author: Insert lead author name here
List content experts here

II. **Endorsement:**

Insert name of Committee Month Year

III. **References:**