Information Security Procedure

Procedure for Policy Exception Requests

Revision 1.0
August 11, 2011
# TABLE OF CONTENTS

1 INTRODUCTION .......................................................................................................................... 1
   1.1 Objective .............................................................................................................................. 1
   1.2 Scope .................................................................................................................................. 1
   1.3 Compliance ........................................................................................................................ 1

2 EXCEPTION REQUEST PROCESS .............................................................................................. 3
   2.1 Making a Request ................................................................................................................. 3
   2.2 Reviewing the Request ........................................................................................................ 3
   2.3 Approving the Request ....................................................................................................... 4
   2.4 Exception Expiration and Re-evaluation ............................................................................ 4
   2.5 Appealing Denied Requests ............................................................................................... 4

3 DOCUMENT ADMINISTRATION ................................................................................................. 5
   3.1 Document Owner ............................................................................................................... 5
   3.2 Document Review ............................................................................................................. 5
   3.3 Change history ................................................................................................................... 5
   3.4 Approval History .............................................................................................................. 5
1 INTRODUCTION

All offices and departments of The New School, and all information systems used by The New School, must comply with The New School Information Security Policy and its associated policies, standards, and procedures. However, circumstances may occasionally arise in which the strict application of a policy, standard, or procedure may not be practical.

1.1 Objective

This process provides a method for requesting, evaluating, and documenting exceptions to compliance with The New School Information Security Policy or any of its associated policies, standards, and procedures.

1.2 Scope

This procedure applies to all offices and departments of the university. This procedure applies only to exceptions to information security policies, standards, and procedures. It does not apply to exceptions to other university policies, standards, or procedures.

1.3 Compliance

Compliance with this procedure is mandatory.
2 Exception Request Process

All offices and departments of The New School, and all information systems used by The New School, must comply with The New School Information Security Policy and its associated policies, standards, and procedures. However, circumstances may occasionally arise in which the strict application of a policy, standard, or procedure may not be practical.

An exception to a policy, standard, or procedure may be requested in any of the following situations:

- A temporary exception is needed because immediate compliance would disrupt critical business operations.
- Another acceptable solution with equivalent protection is available.
- A superior solution is available. An exception may be granted until the solution can be reviewed, and standards or procedures updated to allow the better solution.
- A legacy system is being retired and the cost to remediate the system’s non-compliance issues for the remainder of its lifetime is not justified.
- The cost to remediate the non-compliant systems and/or processes greatly exceeds the cost of non-compliance.
- Resources are not available to implement compliance within the required time frame (in this case, an exception would take the form of an extension of the compliance deadline).

2.1 Making a Request

The Information Owner must acknowledge and approve all requests for exceptions to information security policies, standards, or procedures. The Information Security Office is available for assistance at all stages of this process.

After acknowledging and approving an exception request, the Information Owner or his or her designee must complete and submit an Information Security Policy Exception Request Form to the Information Security Office. The form includes instructions for its completion.

The exception request must include:

- Identification of the applicable part(s) of the policy, standard, or procedure to which an exception is being requested
- The business process or information system for which the exception is being requested
- The information resources used by the business process or information system, and their classifications
- An assessment of the risk(s) incurred as a result of the requested non-compliance
- A description of the compensating controls that will be implemented to mitigate the risk(s)
- An expiration date for the exception.

2.2 Reviewing the Request

Upon receipt of a completed exception request form, the Information Security Office will review the request to identify the risk(s) that would be incurred if the request were approved, and work with the requestor to determine compensating controls that can be implemented to mitigate the risk(s).
2.3 Approving the Request

Depending on the particular details of the request, individuals outside the Information Security Office may be asked to provide additional review and approval:

- In cases where the risk(s) to be incurred involve Confidential information (including student education records and human resources personnel records), the Information Trustee for that information must also approve the request.

- In cases where the risk(s) to be incurred involve Confidential information that will be sent off university premises or provided to a third party, the Office of the General Counsel must also approve the request.

- In cases where the risk(s) to be incurred could have a wider impact than just the business process or information system named in the request, the representatives to the Information Security Steering Committee who represent the impacted areas must also approve the request. If the request will have university-wide impact, it must be approved by the entire Committee.

Approval of the request will not be final until all approvers have signed off, all compensating controls have been implemented, and the Director of Information Security has approved the exception request form.

2.4 Exception Expiration and Re-evaluation

Approved exceptions are valid for a maximum of one year (twelve months) from the date of final approval; shorter expiration dates may be assigned when appropriate. When an exception’s expiration date is approaching, the exception will be re-evaluated to determine whether it is still necessary and, if so, whether it should be renewed and for how long.

2.5 Appealing Denied Requests

Final appeal of denied requests may be made to the Senior Vice President of Information Technology.
3 DOCUMENT ADMINISTRATION

3.1 Document Owner
This document is owned by the Information Security Office, which is responsible for its content and maintenance.

3.2 Document Review
This document is subject to review on an annual (or more frequent, if necessary) basis to validate that its content remains relevant and up-to-date.

3.3 Change history

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial publication</td>
<td>D. Curry</td>
<td>11 August 2011</td>
</tr>
</tbody>
</table>

3.4 Approval History

<table>
<thead>
<tr>
<th>Version</th>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Shelley Reed</td>
<td>SVP, Information Technology</td>
<td>11 August 2011</td>
</tr>
<tr>
<td></td>
<td>Chris Brezil</td>
<td>AVP, Information Technology</td>
<td>11 August 2011</td>
</tr>
</tbody>
</table>
