<Organization Name> Security Investment Policy

1. Overview

<Organization Name>'s purpose for this policy statement is to establish a method of accounting for security investments that will be followed in all cases to determine the ROI of security-related projects. Accounting for security investments is a partially subjective effort, so without consistency the measure becomes meaningless. Employees who are responsible for making, evaluating, or approving security investments should familiarize themselves with the guidelines that follow this introduction.

<Organization Name> will account for all security investments using the Net Present Value (NPV) method. This method is suited for measuring the value of investments with uncertain outcomes, such as security-related investments. Payback, Internal Rate of Return, or other accounting methods not listed here will not be used to evaluate security investments.

At the same time, <Organization Name> recognizes that not every transaction is a purely monetary one. Occasionally, a security-related investment may be so pressing or may have such significant intangible benefits that the investment may be approved even with a negative NPV. On such occasions, the CEO must directly approve the investment.

<Organization name> will take appropriate measures and act quickly in correcting the issue if this policy is violated. Any infractions of this policy will not be tolerated. For questions regarding this policy, contact your supervisor or the accounting department.

2. Purpose

To establish InfoSec responsibilities regarding information security investments, and to define the minimum requirements of an InfoSec investment strategy.

3. Scope

This policy applies to employees, contractors, consultants, temporaries, and other staff at <Organization Name>, including all personnel affiliated with third parties.

4. Policy

4.1. Executive Commitment to Security

4.1.1. Top management within <Organization Name> must set the example. In any business practice, honesty and integrity must be top priorities for executives.

4.1.2. Executives must follow the organization's policy for accounting for security investments.

4.1.3. In accounting for security investments, executives also must comply with all applicable laws and regulations, including, but not limited to, the Sarbanes-Oxley Act, the Federal Information Security Management Act

(FISMA), and the Health Insurance Portability and Accountability Act (HIPAA).

4.1.4. Executives must go beyond the letter of the law and work in the spirit of fair and ethical accounting for security.

4.2. **Employee Commitment to Security**

4.2.1. In accounting for security investments, <Organization Name> employees will comply with all applicable laws and regulations, including, but not limited to, the Sarbanes-Oxley Act, FISMA, and HIPAA.

4.2.2. Employees will strive to help the organization make the most of its investments in security by adhering to organizational policy and playing an active role in securing the enterprise.

4.2.3. Employees will report any questionable accounting transactions to their supervisor or to the accounting department.

4.3. **Organization Awareness**

4.3.1. <Organization Name> will conduct a training program for all new employees who handle security investments to familiarize them with the NPV method of accounting for such investments.

4.3.2. Periodically, <Organization Name> will conduct a training session for existing employees to reinforce the organization's security policy practices, including NPV accounting.

4.4. **Maintaining Consistency**

4.4.1. <Organization Name> will reinforce the importance of consistency in accounting for security, and the tone will start at the top.

4.4.2. Employees at <Organization Name> who have questions about this policy should be encouraged to ask them and to expect timely, honest, objective feedback.

4.5. **Unethical Behavior**

4.5.1. <Organization Name> will avoid the intent and appearance of unethical or compromising practice in accounting for security investments of all types.

4.5.2. <Organization Name> will not permit impropriety at any time, and will act ethically and responsibly in accordance with laws.

5. Enforcement

5.1. Any infractions of this policy will not be tolerated, and <Organization Name> will act quickly in correcting the issue if the policy is violated.

5.2. Any employee or executive found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions

6.1. ROI - Return on Investment: A general term used to describe the net gain or loss resulting from an investment.

6.2. NPV - Net Present Value: A method of determining ROI that takes into account the time value of money.

6.3. Payback: A method of determining ROI that does not take into account the time value of money.

6.4. IRR - Internal Rate of Return: The rate of return a project must achieve to ensure an NPV of zero. Generally, this rate must be greater than the discount rate.
6.5. Discount rate: The rate at which the value of money decreases over a certain period of time (generally a year).