Cyber Security Awareness Assessment Policy

I. PURPOSE

To establish the State of South Dakota policy regarding expectations for state employees to participate in a training program that provides awareness of types of cyber threats, including social engineering and vulnerability exploits.

Technology offers the potential to improve the efficiency and effectiveness of state employees. This benefit includes the responsibility of state employees to protect sensitive government information. Social engineering, email phishing, carelessness, and similar challenges pose risks to the security of the sensitive information stored within the State's Information Technology ("IT") systems. It is important for the State to train employees to recognize the methods used by malicious attackers attempting to gain access to the State's sensitive information. It is equally important the State routinely assess the effectiveness of its training.

II. REFERENCES

BIT's Policy Manual on Training Employees 10.5.4.1
Administrative Rules of South Dakota § 55:10:07:04

III. POLICY STATEMENT

To protect State of South Dakota IT systems from malicious attackers, including those attempting to gain access to the State's sensitive information, each state employee is required to be diligent when using the State's IT systems. Each employee is required to successfully complete annual cyber security training provided by the Bureau of Information and Telecommunication ("BIT"). In addition, an employee who has access to certain classes of protected data will be provided a specific training program that brings awareness of federal policies regarding requirements to protect each class of data and to report security breaches.

Each employee shall be aware of the tactics used in social engineering, phishing, and similar tactics used to gain unauthorized access to the State's IT system. Social engineering is the use of psychological manipulation to trick an employee into providing confidential information to an unauthorized individual. In addition, emails provide easy, convenient access to an employee by a malicious attacker. Each employee must take the necessary steps to protect the State's IT systems from such attacks.

IV. POLICY SCOPE

All state employees under the purview of the Governor are subject to the requirements of this policy. Failure by an employee to comply with the requirements of this policy may lead to disciplinary action.

V. POLICY IMPLEMENTATION

1) Each employee shall successfully complete annual cyber security training approved or provided by BIT, which will provide the employee enough information to understand various attack

methods. Training will include information regarding the dangers of social engineering, data protection requirements, recognition of phishing emails, and tips on how to protect the State's systems from such threats. Failure to successfully complete the assigned training may result in disciplinary action or other remedial action to ensure the employee completes the necessary training.

2) Employees have the responsibility to recognize and report suspicious situations; if you see something, say something. Phishing or spam email messages, unknown IT personnel, unexpected computer support phone calls, individuals loitering near secured facilities, and "conveniently found" thumb drives are examples of situations that should be reported to the BIT Help Desk.

   All BIT employees are provided a photo identification badge. A state employee may attempt to substantiate the identification of any unknown individual claiming to be a BIT employee by looking at the individual's photo on the email Global Address List or by contacting the BIT Help Desk for confirmation.

3) An employee who loses state technology assets (i.e. a laptop computer, access security card, etc.) or sensitive state data must notify the employee's supervisor and the BIT Help Desk immediately.

4) At least annually, BIT will test each employee with a cyber awareness exercise. Each employee is expected to use the skills provided during the IT security training to recognize social engineering, phishing emails, unknown personnel, and other security tests. Phishing messages should either be deleted or reported to BIT's Report Spam email address (ReportSpam@state.sd.us). Other security tests should be reported to the BIT Help Desk.

   a. An employee initially failing a security awareness assessment will be directed to an educational tutorial explaining how the employee should have identified the situation as a potential threat to the State's system. The employee will be subject to an additional assessment during the subsequent months.

   b. An employee failing a second security awareness assessment during a rolling twelve-month period will be directed to an educational tutorial explaining how the employee should have identified the situation as a potential threat to the State's system. In addition, the employee will be contacted by a BIT employee who will explain the importance of cybersecurity and suggest how the employee may identify these risks. The employee's supervisor will be notified that the employee failed a second security awareness assessment. The employee will be subject to an additional assessment during the subsequent months.

   c. An employee failing a third security awareness assessment during a rolling twelve-month period will be directed to an educational tutorial explaining how the employee should have identified the situation as a potential threat to the State's system. In addition, the employee will be required to attend on-site cybersecurity training presented by BIT. The employee's supervisor will be notified that the employee failed a third security assessment. Lastly, the employee will be subject to an additional assessment during the subsequent months.

   d. An employee failing a fourth security awareness assessment during a rolling twelve-month period will be subject to disciplinary action. The employee will receive a written reprimand from the agency for failing to properly utilize the provided IT security training. In addition, BIT will contact agency management and the employee to discuss further remedial solutions to ensure the employee properly understands the importance of cybersecurity. The employee will be required to attend on-site cybersecurity training presented by BIT.

e. An employee failing a fifth security awareness assessment during a rolling twelve-month period will be subject to further disciplinary action. The employee will be suspended without pay for three days and receive a last chance letter. In addition, BIT will contact agency management and the employee to discuss further remedial solutions to ensure the employee properly understands the importance of cybersecurity. The employee will be required to attend on-site cybersecurity training presented by BIT.

f. An employee failing a sixth security awareness assessment during a rolling twelve-month period may be disciplined, up to and including termination.