Mississippi State University Information Security Program
Training and Awareness

1. **Purpose:** The purpose of this section is to define the training and awareness program as an element of the Mississippi State University Information Security Program.

2. **Scope:** This program applies to the handling of sensitive information by employees and students of Mississippi State University.

3. **Program:** A key component of the university's Information Security Program is training and awareness on the part of the people entrusted with collecting and handling sensitive information. The university has an additional obligation to educate its students and employees about the importance of protecting their own personal information. Therefore the Training and Awareness section of the Information Security Program has two goals, the first to educate all employees on proper protection of sensitive information and the second to teach students, faculty and staff to protect their own personal information.

3.1. **Training:** The first major element of the training and awareness program is online training aimed at employees, graduate assistants, and student workers. The training is organized in a modular format to facilitate progression through the material, and each module ends with a quiz that measures understanding of the material just covered. Once an individual completes all required modules, that person is certified to have successfully completed the required MSU information security training. This certification is good for a period of two years.

All employees in the following EEO categories are required to complete information security training:

- EEO 10 – Executive/Administrative and Managerial
- EEO 20 – Faculty
- EEO 30 – Professional (non-faculty)
- EEO 40 – Technical and Paraprofessional
- EEO 50 – Clerical and Secretarial

All graduate assistants are also required to complete the training. Employees in other EEO categories and student workers may be required by their unit head to take the training.

Those required to have information security training must successfully complete it within 30 days to receive their two-year information security training certification. After two years, the training must be retaken and completed, again within 30 days, to maintain certification for another two years. Individuals who are within their 30 day training window will receive email notification of their requirement to complete the training, along with instructions on how to access the training materials.

It is the responsibility of unit heads to ensure that employees in the above EEO categories and graduate assistants complete the information security training. It is also the responsibility of unit heads to ensure that employees not in the above EEO categories and student workers who have access to sensitive information complete the training as appropriate. Employee orientation will be used to inform new personnel about the program and the requirement to complete training within 30 days of employment. Information security training records will be maintained to indicate who has completed the training and when, and a report will be available to unit heads to track compliance. Internal Audit will confirm compliance during departmental audits.

The Information Technology Council is responsible for periodic review of the information security training content and for recommending changes to ensure continued relevance and effectiveness.

3.2. **Awareness Campaign:** The second major element of the training and awareness program is a campaign targeted at student and employee protection of one's own personal information. The campaign will use a combination of informational Web sites, student awareness sessions during Freshmen Orientation, printed brochures, and posters. The content of these different types of media will focus on the importance of individuals protecting themselves by securing their personal information. Examples relevant to students such as their activities on social networks like Facebook will be used. Additionally, protection of important personal university credentials such as the MSU ID Card and NetPassword will also be stressed.

3.3. **Cyber Security Awareness Week:** The third major element of the training and awareness program is a Cyber Security Awareness Week which will be an annual event held during the fall semester. The event will employ a variety of resources such as information booths, seminars, and demonstrations. Specific aspects of information security such as identify theft will be highlighted, and information security experts from across campus will be employed. The goal of the Cyber Security Awareness Week is to provide a periodic reminder to the campus of the importance of information security, thus maintaining a high level of awareness among faculty, staff, and students.

4. **Summary:** Information security is a shared responsibility that cuts across all segments of the university. A number of units are collaborating to develop and implement the university's training and awareness component of the Information Security Program. Participating units include the Department of Human Resources Management, Dean of Students, Information Technology

Services, and the computer security program in Computer Science and Engineering.