Guidelines for protecting the confidentiality of Social Security Numbers (SSN)

WCU personnel are expected to collect, use, and maintain social security numbers only in situations where there are legal or other legitimate business reasons to do so.

The following business practices should be adopted to ensure the appropriate protection of the confidentiality of social security numbers.

Reduce the use and collection of social security numbers (SSNs)
Use and collect SSNs only when required to do so by law or where there are other legitimate business reasons to do so. Normally, SSNs should not be used as primary identification numbers. Employees should be advised to use other identifiers (such as payroll employee ID numbers) on forms that previously may have required SSNs (such as leave request forms). SSNs should be collected and used only as reasonably necessary for the proper administration of lawful business activities.

Inform Individuals when the campus collects SSNs
WCU personnel must inform individuals of the purpose of the collection and intended use of their SSNs, whether there is a legal requirement to collect, and the consequences of not providing the SSNs.

Eliminate the public display of SSNs
WCU personnel should take appropriate steps to ensure that SSNs are not placed on documents widely seen by others. Except as required by law, documents with SSNs should not be sent through the mail. If documents that require SSNs are mailed, WCU employees must ensure that the SSNs are not revealed by window envelopes. When using electronic media, avoid sending SSNs and send only necessary SSNs with encryption or a secure connection. Suggesting or requiring the use of SSNs as passwords or codes for access to internet web sites or other services should be eliminated.

Control access to SSNs
WCU personnel should limit access to SSNs to only those employees with a legitimate need for performance of their duties. Regular monitoring or auditing should occur to ensure access is appropriate. Records with SSNs should be protected when in manual or electronic storage or back-up through locked cabinets or encrypted files. SSNs should not be stored on electronic equipment without secured access. SSNs only should be shared with other organizations where required by law or where there is a legitimate business need and there is a legal agreement in place to protect the confidentiality of SSNs.

Protect SSNs with security safeguards
WCU personnel should have a security plan for record systems that contain SSNs and written policies for protecting the confidentiality of SSNs. These policies should specify actions that employees must take to protect the confidentiality of SSNs (such as requirements for securing, using and destroying records with SSNs) and to report promptly any inappropriate disclosure or loss of records containing SSNs.

Accountability for protecting SSNs
At a minimum, all departments and divisions should provide training for employees on their responsibility for protecting SSNs, impose discipline on employees for non-compliance and conduct risk assessments and audits of record systems containing SSNs.