Policy 909

1 Introduction

1.1 The purpose of this policy is to allow Network Infrastructure and Control Systems or designated security officer to perform periodic information security network risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2 Scope

2.1 Risk assessments can be conducted on any entity within Appalachian State University or any outside entity that has signed a Third Party Agreement with Appalachian State University. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3 Definitions

3.1 Entity

Any business unit, department, group, or third party, internal or external to Appalachian State University, responsible for maintaining Appalachian State University assets.

3.2 Risk

Those factors that could affect confidentiality, availability, and integrity of Appalachian State University's key information assets and systems. The Risk Assessment Team is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets on Appalachian networks, while minimizing the impact of security procedures and policies upon business or educational missions.

4 Policy and Procedure Statements

4.1 Policy

4.1.1 The execution, development and implementation of remediation programs is the joint responsibility of Network Infrastructure and Control Systems, the Information Security Officer and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Risk Assessment Team in the development of a remediation plan.

4.2 Risk Assessment Process

4.2.1 For additional information, contact Network Infrastructure and Control Systems or the Information Security Officer.

4.3 Enforcement

4.3.1 Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

5 Additional References

6 Authority

7 Contact Information

8 Original Effective Date

This policy was approved by the Provost on July 19, 2005

9 Revision Dates