Association of Clinical Research Professionals
Finance Committee Policy 4.8

Information Security: Vulnerability and Threat Management Policy

Purpose
The purpose of the *Information Security: Vulnerability and Threat Management Policy* (the "Policy") is to ensure that vulnerabilities and threats to the operating system or environment for information systems are identified, corrected, or mitigated to minimize the risks associated with them. ACRP recognizes that the establishment and implementation of effective data integrity controls procedures is a crucial element in providing reasonable protections to the personal and proprietary data of the Association of Clinical Research Professionals (ACRP) and its "customers" (members, affiliates, business partners and other groups or individuals engaged with the business of the association.)

Authority
The Executive Director is responsible for assessing the vulnerability and for managing potential to the data security of ACRP and its customers.

Administration
The Executive Director and Senior Director, Operations shall be responsible for developing, implementing and revising this policy in consultation with technology staff and/or IT consultants.

Policy

Personally Identifiable Information (PII)

'PII' is used in this and all ACRP Security Policies. It is defined as: 'Any data, including financial information, that could potentially identify a specific individual.'

Regular Vulnerability Assessments

Through a third-party vendor or IT management contractor ACRP will regularly monitor potential vulnerability to the PII of ACRP and its customers in the following ways:

1. Perform automated vulnerability assessments and continuously monitor threats against ACRP web applications.

2. Conduct vulnerability scans against critical infrastructure components (servers, switches, routers, etc.) at least monthly or when significant changes to the environment are made.

3. Review the resulting report after each vulnerability test and have a remediation plan (excluding

false positive results) regardless of risk level within 24 hours.

4. Re-run the vulnerability test after risks have been remediated to prove that all risks are resolved.
5. Electronically monitor (24/7) all attacks and potential threats.

Documentation

Through its third-party vendor or IT management contractor, ACRP will fully document all patch management and system update-related procedures, activities, and efforts to mitigate future risk and to maintain for historic reference.

MONITORING AND REVIEW SCHEDULE
Review every three years or as needed by the Executive Director, Senior Director, Operations in consultation with technology staff and/or IT consultants.

DATES REVIEWED
December 13, 2017 (By ABoT)

DATES MODIFIED
December 13, 2017 (By ABoT)

DATES APPROVED
December 13, 2017 (By ABoT)