Personally Identifiable Information

Scope

This document establishes policy, definitions and guidance for the protection of Personal Identifiable Information (PII) for the Boy Scouts of America (BSA).

Background

This document provides the procedures in use at Boy Scouts of America (BSA) to implement policies about protecting personally identifiable information (PII). While it is expected that physical versions of documents containing PII will be protected in similar ways, these procedures apply only to electronic copies of PII.

Applicability

This policy is applicable to all BSA employees at National Council, Regions, Scout Shops, Local Councils and NDC locations.

Definition of PII

At BSA, PII is defined as an individual's full name in combination with one or more of the following items:

- *Personal Information:*
  Social Security number or foreign national identification number, date and place of birth, passport or visa number, driver's license number, detailed medical records, security background information & mother's maiden name.
- *Financial Information:*
  Bank name and account number(s) and associated PIN numbers.
- *Business Information:*
  Employee number along with salary information.
- *Consumer Information:*
  Credit card numbers and associated PIN numbers, credit history reports, automobile insurance cards and or certificates.

This list will be periodically reviewed by the Boy Scouts of America Human Resources Department and changes will be communicated to all employees.

PII Policy

As a general rule, individuals are not permitted to have any Protected PII on their computers or in data on general use servers. Protected PII is restricted to the specific systems discussed below, each of which is contained within a moderate level Major Application (MA). (Note: a Major Application is a lab defined collection of computing systems with a common set of risks and security procedures, generally more stringent than the lab baseline. Moderate level specifies a set of NIST defined security controls, again more stringent than the lab baseline.)

There are two separate types of Protected PII containing systems. The first, called "Enterprise Protected PII systems", maintains Protected PII that needs to be accessed from other systems and individuals around the laboratory, normally over the lab network. The second, called "Local Protected PII systems", maintains Protected PII that is only needed by a small number of individuals who can access the system directly, not over the network.