Carnegie Mellon University
Software Engineering Institute

ITPE SUGGESTED DOCUMENTS LIST

Introduction

This note provides a starting point to help an organization provide documents necessary for starting an assessment. Some organizations will have these documents on their internal website, so they mayneed to provide screen captures. Others may combine several of the suggested documents into larger documents.

1) Org chart for InTP with roles
2) Overall org chart for whole organization
3) Any CONOPs or charter for the InTP
4) Any organizational materials describing the InTP
5) Authority for Insider Threat Program
6) Any policies describing the InTP
7) Other related policies
   a) Acceptable Use Policy
   b) Insider Threat Incident Handling Policy or Plan
   c) General Incident Response Plan
   d) Intellectual Property Agreements
   e) Right to Privacy (most companies and agency clearly state that the employee has NO privacy when using agency IT systems)
   f) Email use policy (if different from AUP above)
   g) Internet use policy (if different from AUP above)
   h) Data Handling Policy and Procedures (includes Data Classification policy)
8) Procedures or practices or policies related to
   a) HR Process for Disciplinary Action and Employee Separation Handling
   b) Account access and authorization and termination process
   c) User monitoring policies or banners
9) List of data sources collected for analysis
   a) Behavioral
   b) Technical
   c) Counterintelligence and personal security
   d) Physical security
10) Description of any data analysis mechanisms and processes (Analytic Hub or similar mechanism)

11) Description of how data is collected and analyzed for the InTP
12) Defined roles and responsibilities for Insider Threat Program Team.
13) Any announcements, memos, support from Executive Management about the InTP
14) Any description of employee assistance or workplace violence programs
15) Insider Threat Training Materials and Plan
    a) For employees in general
    b) For InTP team members
16) Sample contract wording with business partners or supply chain partners or agreements with contractors and sub-contractors related to reporting security incidents, termination of employees, acceptable use behaviors, or data protection

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0883

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu