

ITPE SUGGESTED DOCUMENTS LIST

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

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 may need 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

Copyright 2023 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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