

# PP-Module for Redaction Tools



Version: 1.0-Draft  
2022-04-29

**National Information Assurance Partnership**

# Revision History

| Version   | Date       | Comment             |
|-----------|------------|---------------------|
| 1.0-Draft | 2022-04-29 | Initial publication |

# Contents

- 1 Introduction
  - 1.1 Overview
  - 1.2 Terms
    - 1.2.1 Common Criteria Terms
    - 1.2.2 Technical Terms
  - 1.3 Compliant Targets of Evaluation
    - 1.3.1 TOE Boundary
  - 1.4 Use Cases
- 2 Conformance Claims
- 3 Security Problem Description
  - 3.1 Threats
  - 3.2 Assumptions
- 4 Security Objectives
  - 4.1 Security Objectives for the TOE
  - 4.2 Security Objectives for the Operational Environment
  - 4.3 Security Objectives Rationale
- 5 Security Requirements
  - 5.0.1 Security Audit (FAU)
  - 5.0.2 User Data Protection (FDP)
  - 5.0.3 Protection of the TSF (FPT)

1.0-Draft National Information Assurance Partnership 2022-04-29 Redaction 1.0-Draft 2022-04-29 Initial publication

# 1 Introduction

## 1.1 Overview

The scope of this Protection Profile Module (PP-Module) is to describe the security functionality of redaction tools in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- Protection Profile for Application Software, Version 1.4 (App PP or PP\_APP\_V1.4)

This Base-PP is valid a redaction tool is a specific type of software application and can therefore be reasonably expected to implement security functionality that is typical of application software. Redaction is the process of selectively removing and replacing information from a document or other logical container of data for release to an audience not intended to view that information. Redacted information is not limited to classified material; other examples include privacy data, proprietary information, trade secrets, and legal strategy. Instances of redaction include replacing classified text with a black box to release a document to an unclassified environment, replacing privacy-related data such as telephone numbers with all Xs to release a database to a contractor, converting a proprietary format document to Portable Document Format (PDF) to release a what-you-see-is-what-you-get (WYSIWYG) document. The risk from improper or incomplete redaction is the inadvertent disclosure of classified or sensitive data.

Redaction is not sanitization. In the sanitization process, information is removed with no indication that the sanitization process took place. In the redaction process, selected visible information is removed and replaced with something innocuous (e.g. black box or text) so that the reader knows redaction took place. This replacement is a critical part of the process not shared with sanitization. Redaction is not sanitization. In the sanitization process, information is removed with no indication that the sanitization process took place. In the redaction process, selected visible information is removed and replaced with something innocuous (e.g. black box or text) so that the reader knows redaction took place. This replacement is a critical part of the process not shared with sanitization.



**Figure 1: Figure 1: One possible workflow of an electronic document through the redaction process.**

Figure 1 shows the typical workflow of a document from source to destination and through the redaction process. Other workflows are possible. Software vendors have the flexibility to devise their own workflow solutions for their target consumer. However, in any workflow, this PP-Module applies only to the part of the workflow that is performed by the redaction tool and only to the redaction functionality in that tool. Other functionality in the redaction tool, other tools used in the workflow, the organization's redaction policy as well as security requirements and security policies that apply to other parts of the workflow are beyond the scope of this PP-Module.

## 1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

### 1.2.1 Common Criteria Terms

|  |   |
|--|---|
| Assurance                              | Grounds for confidence that a TOE meets the SFRs [CC].  |
| Base Protection Profile (Base-PP)      | Protection Profile used as a basis to build a PP-Configuration.   |
| Collaborative Protection Profile (cPP) | A Protection Profile developed by international technical communities and approved by multiple schemes. |

|   |   |
|---|---|
| Common Criteria (CC)                                | Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).  |
| Common Criteria Testing Laboratory                  | Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations. |
| Common Evaluation Methodology (CEM)                 | Common Evaluation Methodology for Information Technology Security Evaluation.   |
| Distributed TOE                                     | A TOE composed of multiple components operating as a logical whole.   |
| Extended Package (EP)                               | A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.   |
| Functional Package (FP)                             | A document that collects SFRs for a particular protocol, technology, or functionality.  |
| Operational Environment (OE)                        | Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.   |
| Protection Profile (PP)                             | An implementation-independent set of security requirements for a category of products.  |
| Protection Profile Configuration (PP-Configuration) | A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.   |
| Protection Profile Module (PP-Module)               | An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.   |
| Security Assurance Requirement (SAR)                | A requirement to assure the security of the TOE.  |
| Security Functional Requirement (SFR)               | A requirement for security enforcement by the TOE.  |
| Security Target (ST)                                | A set of implementation-dependent security requirements for a specific product.   |
| Target of Evaluation (TOE)                          | The product under evaluation.   |
| TOE Security Functionality (TSF)                    | The security functionality of the product under evaluation.   |
| TOE Summary Specification (TSS)                     | A description of how a TOE satisfies the SFRs in an ST.   |

### 1.2.2 Technical Terms

|                 |   |
|-----------------|---|
| Attachments     | An electronic document or data file that is part of the main file but is logically distinct and separable from the main electronic document.  |
| Complex Objects | Objects that may have their own static or functional metadata and may differ between the stored and visible form, such as images, attachments, Microsoft OLE objects, Microsoft ActiveX controls, and temporal objects. |
| Functional data | Forms, scripts, link Uniform Resource Locators (URLs), workflow data, action buttons, formulas in a spreadsheet, macros or any type of executable content.  |
| Images          | The actual image data stored in the file as opposed to what is visible; the visible image can be  |

|   |  |
|---|--|
|   | cropped or resized but the full image could still be retained in the file format and may or may not match the visible image; some image formats can have their own metadata, such as Joint Photographic Experts Group (JPG) and Tagged Image File Format (TIFF).   |
| Metadata of objects or embedded objects | Data associated with an object to describe or identify the contents of the object such as exchangeable image file format (EXIF) data of images; images themselves can contain other images and their own metadata.   |
| Obscured visible data                   | Content that could be visible but is obscured in some way such as content that runs off an edge of the container, text in a black font on black background (or any color of font on a similar color background), very small fonts, cropped or clipped graphics or images, hidden layers, portions of an embedded object (e.g. Microsoft Object Linking and Embedding (OLE)) that are outside the view container. |
| Remnant data                            | Artifacts of the original application or source file format such as remnant or unreferenced data from fast saves, unreferenced or unused elements, malformed elements that cannot be fixed, garbage data in the file structure.  |
| Static data or metadata                 | File properties such as author or creation date, stored form field data, undo cache or any data kept to revert to a prior version of an element or the document itself, incremental updates, collaboration data such as comments, tracked changes, workflow data, embedded search indexes, bookmarks, document info added by 3rd-party apps, accessibility data such as alternate text, etc.                     |
| Structural data                         | Data that is part of the file format structure, such as a file header or fonts, and is necessary to interpret the file properly for display or print.  |
| Temporal Objects                        | A particular type of complex object whose representation extends through a time interval, such as video, audio, flash animation, slide shows, etc. References to “complex objects” in the requirements section of this paper include temporal objects.   |
| Visible contents                        | The visible contents of the file; the visual representation of text, images and complex objects.   |

## 1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) described by this PP-Module is limited to the redaction of electronic documents defined in standards such as the series International Organization for Standards (ISO)/International Electrotechnical Commission (IEC)-29500 (Office OpenExtensible Markup Language (XML), e.g. Microsoft Word, PowerPoint, and Excel documents) and ISO/IEC-32000 (PDF), or the definitive standard for a format. Mail guards, filters, and batch redaction tools are beyond the scope of this PP-module. Requirements that apply to features such as administrative control over particular redaction settings, multi-person review prior to release, etc., are outside the scope of this PP-Module. The TOE may have those features but is not required to have them and their use and enforcement is governed by the organization’s redaction policy.

This PP-Moudle covers the software functionality of the redaction process; it does not include requirements for how users should decide what to redact or other policy issues. Analysis of documents for covert data transfer is part of the decision-making process for what to redact and so occurs prior to the redaction itself. The requirements in this document are independent of requirements levied on document release by statute or the judiciary.

Data execution risks inherent in some file formats are beyond the scope of this PP-Module. This PP-Module assumes that scanning for such risks occurs prior to the document entering the redaction functionality of the TOE.

Documents to be redacted may contain objects that are vulnerable to steganography, such as images or video. Functional data such as scripts can contain strings or images that may not be accessible to the redaction tool. Analysis of such objects for attacks or covert data transfer will occur outside of the redaction process. An organization’s security policy will determine whether such objects are released or redacted in their entirety.

### 1.3.1 TOE Boundary

The physical boundary for a TOE that conforms to this PP-Module is a software application that installed on top of a general-purpose or mobile operating system. The TOE’s logical boundary includes all functionality required by the claimed Base-PP as well as the redaction functionality and related capabilities that are defined in this PP-Module. Any functionality that is provided by the application that is not relevant to the security requirements defined by this PP-Module or the Base-PP is considered to be outside the scope of the TOE.

## 1.4 Use Cases

Redaction Tools perform tasks associated primarily with the following use case.

## **[USE CASE 1] Content Redaction**

Redaction tools are used for the redaction of user selected content from a document.

# 2 Conformance Claims

## Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PPs and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

## CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (extended) of Common Criteria Version 3.1, Revision 5 [CC].

## PP Claim

This PP-Module does not claim conformance to any PP.

## Package Claim

This PP-Module does not claim conformance to any packages.

# 3 Security Problem Description

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment (OE), and any organizational security policies that the TOE is expected to enforce.

## 3.1 Threats

---

The following threats defined in this PP-Module extend the threats defined by the Base-PP.

### **T.CLUES\_TO\_ORIGINAL\_DATA**

Text or graphics placed in the redacted area by the TOE may contain clues to the nature of the original redacted information.

### **T.UNREDACTED\_DATA**

A failure of the redaction tool to remove user selected visible or hidden data could result in the inadvertent dissemination of information.

## 3.2 Assumptions

---

These assumptions are made on the Operational Environment (OE) in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an OE that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality. This PP-Module defines assumptions that extend those defined in the supported Base-PP.

### **A.KNOWLEDGEABLE\_USER**

The user is knowledgeable concerning document management and has appropriate training with the redaction tool. Part of this knowledge and training includes how to prepare a document for the redaction tool, e.g. resolve and turn off tracked changes prior to redaction, work with a copy of the document and preserve the original file, remove passwords and decrypt files, etc.

### **A.INFORMATION\_RELEASE\_POLICY**

There is a redaction or information release policy in place for the organization which the user follows.

### **A.PRESERVE\_DOCUMENT\_LAYOUT**

The TOE will preserve the layout of the document.



# 4 Security Objectives

## 4.1 Security Objectives for the TOE

---

**O.INSPECTION**

The TOE will analyze the file content for metadata and elements, to include any that are purposely hidden or not immediately visible to the naked eye. This metadata and elements includes, but is not limited to those that are obstructed from view such as shapes on top of text, hidden objects (manual direct formatting or programmatically hidden), and text that is positioned off the margins, and/or is located in header and footer sections of the file.

**O.MANAGEMENT**

placeholder

**O.QUALITY**

placeholder

**O.REDACTION**

The TOE will provide the capability to completely remove any data selected for redaction.

**O.REPORT**

The TOE will provide the capability to produce a report of all data redacted and any errors during redaction.

## 4.2 Security Objectives for the Operational Environment

---

The OE of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). The security objectives for the OE consist of a set of statements describing the goals that the OE should achieve. This section defines the security objectives that are to be addressed by the IT domain or by non-technical or procedural means. The assumptions identified in Section 3 are incorporated as security objectives for the environment. This PP-Module defines environmental security objectives that extend those defined in the supported Base-PP.

**OE.PLACEHOLDER**

placeholder

## 4.3 Security Objectives Rationale

---

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 1: Security Objectives Rationale

| Threat, Assumption, or OSP   | Security Objectives | Rationale   |
|------------------------------|---------------------|-------------|
| T.CLUES_TO_ORIGINAL_DATA     | O.PLACEHOLDER       | placeholder |
| T.UNREDACTED_DATA            | O.PLACEHOLDER       | placeholder |
| A.KNOWLEDGEABLE_USER         | OE.PLACEHOLDER      | placeholder |
| A.INFORMATION_RELEASE_POLICY | OE.PLACEHOLDER      | placeholder |
| A.PRESERVE_DOCUMENT_LAYOUT   | OE.PLACEHOLDER      | placeholder |

## 5 Security Requirements

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, with additional extended functional components.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignments are indicated with *italicized* text.
- Refinements made by the PP-Module author are indicated with **bold text** for added or substituted text and ~~striktthrough~~ text for removed text. Refinements are only applied to significant technical changes to existing SFRs; minor presentation changes with no technical impact (such as British vs American spelling differences) are not marked as refinements. Refinements are also indicated when an operation is added or substituted for an existing operation (e.g. the PP-Module completes an assignment in such a way that it introduces a selection into the assignment).  
Note that for SFRs that are defined either in CC Part 2 or in this PP-Module's Extended Components Definition, the refinement operation is used to indicate deviations from the defined component. For Base-PP SFRs that are modified by this PP-Module, the refinement operation is used to indicate deviations from the Base-PP's definition of the SFR (i.e. if the Base-PP refined an SFR and that change is not affected by this PP-Module, it is not shown here as a refinement).
- Selections are indicated with *italicized* text.
- Iteration is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration, e.g. 'VPN' for an SFR relating to VPN gateway functionality.
- Extended SFRs are identified by having a label "EXT" after the SFR name.

Note that selections and assignments to be completed by the ST author are preceded with “selection:” and “assignment:”. If text is italicized and does not include either of these, it means that the selection or assignment has already been completed in this PP-Module and the ST author must use the text as written.

<https://raw.githubusercontent.com/commoncriteria/application/master/input/application.xml>

<https://www.niap-cc-evs.org/Profile/Info.cfm?PPID=442&id=442>

Placeholder When this PP-Module is used to extend the App PP, the TOE type for the overall TOE is still a software application. The TOE boundary is simply extended to include redaction functionality that is provided by the application. The threats, assumptions, and organizational security policies (OSPs) defined by this PP-Module (see sections 3.1 through 3.3) supplement those defined in the App PP as follows:

Placeholder Placeholder Placeholder Placeholder Placeholder Placeholder Placeholder

### 5.0.1 Security Audit (FAU)

## FAU ALR EXT.1 Redaction Failure Notification

FAU ALR EXT.1.1

The TOE must make the user aware when redaction fails for any reason.

## Evaluation Activities

*FAU ALR EXT.1*

***TSS***

*The evaluator shall examine the TSS to ensure it describes how the TOE notifies the user when redaction fails. The evaluator shall ensure that the TSS' description complies with the requirement that the user is notified when redaction fails for any reason.*

## Guidance

*There are no guidance EAs for this component.*

## Tests

*The evaluator shall acquire or create test files that should fail the redaction, apply the TOE and verify that the TOE alerts the user that the redaction failed.*

## FAU REP EXT.1 Report Generation

FAU REP EXT.1.1

The TOE must be able to generate a report entry that contains metadata about each element that was redacted, including at least the following: the type of the element that was removed, the location if it was a visible element, and whether the element was selected by the user or removed automatically.

**Application Note:** The report can be a configurable feature that is only generated on user request. Location can be a page number, a cell number for a spreadsheet, or some other indication that allows the user to easily locate the visible element.

## Evaluation Activities ▼

### [FAU\\_REP\\_EXT.1](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure it describes the TOE's reporting feature and the metadata that is included for each report entry.*

#### **Guidance**

*The evaluator shall examine the operational guidance to ensure it contains instructions for the configuration of the reporting feature in accordance with this requirement.*

#### **Tests**

*The evaluator shall create test files with specific elements to redact, apply the TOE to the test files, and observe that there is a report for each element expected to be redacted. This assurance activity can be done in conjunction with [FAU\\_SAR\\_EXT.1](#).*

## **FAU\_SAR\_EXT.1 Report Review**

### FAU\_SAR\_EXT.1.1

The TOE must allow the user to access a report of the data that was redacted.

**Application Note:** This can be satisfied with a dialog box or other simple list of items that were redacted. The report can be a configurable feature that is only generated on user request.

## Evaluation Activities ▼

### [FAU\\_SAR\\_EXT.1](#)

#### **TSS**

*There are no TSS EAs for this component.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create test files with specific elements to redact, apply the TOE to the test files, and observe that there is a report entry for each element expected to be redacted.*

## **5.0.2 User Data Protection (FDP)**

### **FDP\_DID\_EXT.1 Identification of Data**

#### FDP\_DID\_EXT.1.1

The TOE must identify all hidden data in the document, except remnant data and undo or tracked change buffers, and allow the user to review and select each hidden data element individually for redaction.

**Application Note:** Remnant data and undo or tracked change buffers are removed automatically according to [FDP\\_RIP\\_EXT.1](#). If the file or part of the file is encrypted, the TOE will have to reject the file or decrypt it so that the tool and the user can review the hidden data.

#### FDP\_DID\_EXT.1.2

The TOE must identify all obscured data and must [**selection:** *remove the obscured data automatically, allow the user to redact the obscured data*].

**Application Note:** Obscured data is anything that could be visible but is obscured in some way, such as the cropped portion of an image or graphic. While the user sees only the portion of the graphic in the view container, the document contains the data in the cropped area. The tool must either remove the obscured data automatically or give the user the choice to remove or retain the obscured area.

#### FDP\_DID\_EXT.1.3

The TOE must identify images where the visible representation is reduced in size or resolution from the representation stored in the file format and must [**selection:** *automatically replace the stored data with the visible representation, allow the user to replace the stored data with the visible representation, allow the user to leave the image unaltered*].

**FDP\_DID\_EXT.1****TSS**

*The evaluator shall examine the TSS to ensure it specifies the hidden data that it identifies and allows the user to select for redaction. The evaluator shall ensure that the TSS' description complies with the requirement for the TOE to identify all hidden data and allow the user to review and select each hidden data element for redaction.*

*The evaluator shall examine the TSS to ensure it describes how the TOE handles all obscured data. The evaluator shall ensure that the TSS' description complies with the requirement that all obscured data is identified and either removed automatically or redacted by the user.*

*There are no TSS EAs for this element.*

**Guidance**

*There are no guidance EAs for this element.*

*There are no guidance EAs for this element.*

*There are no guidance EAs for this element.*

**Tests**

*The evaluator shall create test documents with various types of hidden data apply the TOE, and verify that it identifies each expected element and allows the user to select and redact each. The evaluator shall create test documents with various forms of obscured data, apply the TOE, and verify that the tool identifies the obscured data and either removes the obscured data automatically or gives the user the choice to remove or retain the obscured data. The evaluator shall create a test document with an image that is stored in a larger size and resolution than the visible image and apply the TOE without selecting the image for redaction. The evaluator shall verify that the TOE either*

- gives the user a choice to retain the image unaltered or replace the stored data with the visible data. For the choice to replace the image, the evaluator shall examine the output file to locate the image and verify its size and resolution, or extract the image with an appropriate tool for that format and compare the size and resolution of the extracted image to the visible image to determine if they match.*
- resizes the stored image. To determine this, the evaluator shall examine the output file to locate the image and verify its size and resolution, or extract the image with an appropriate tool for that format and compare the size and resolution of the extracted image to the visible image to determine if they match.*

**FDP\_DIN\_EXT.1 Deep Inspection****FDP\_DIN\_EXT.1.1**

For each element of the file format that can contain its own metadata, other elements, or hidden data, the TOE must [**selection:** *recurse through the element chain and apply the PP to each layer, simplify the element, redact the element*].

**Application Note:** For example, JPG images can contain metadata called EXIF data. Some image formats can contain the same image in another format, such as raw which can contain a complete jpg version of the image. A complex object can contain other complex objects (e.g. Microsoft OLE). The tool must apply the requirements to each layer of every element and identify hidden/metadata not just at the top layer of the document but in each element and in all layers within that element. If the TOE cannot recurse through the layers, it must simplify the element at the top level.

**FDP\_DIN\_EXT.1****TSS**

*The evaluator shall examine the TSS to ensure it lists and describes the methods used to replace redacted elements that contain metadata, other elements, or hidden data. The evaluator shall ensure that the TSS' description complies with the requirement that each element is handled by either recursing through the element chain and applying the TOE to each layer, simplifying the element, or redacting the element.*

**Guidance**

*There are no guidance EAs for this component.*

**Tests**

*The evaluator shall create or acquire test files that contain elements that themselves contain*

*other elements and hidden data. The evaluator shall examine the document to identify these elements in the structure, apply the TOE, and examine the output to verify that the elements were handled properly via either redaction or simplification in accordance with the requirement.*

## **FDP\_LOC\_EXT.1 Redact Content from Every Location**

FDP\_LOC\_EXT.1.1

The TOE must remove redacted content from every location in the file format where it is stored.

### **Evaluation Activities** ▼

[\*FDP\\_LOC\\_EXT.1\*](#)

#### **TSS**

*There are no TSS EAs for this component.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create or acquire test files that contain content in multiple places and examine the files to locate the content. The evaluator shall apply the TOE and examine the output to verify that it has been removed from every location.*

## **FDP\_NND\_EXT.1 No New Data Introduced by TOE**

FDP\_NND\_EXT.1.1

The TOE itself must not introduce new hidden data that was not requested by the user without warning the user of the addition.

**Application Note:** If the redaction process changes the format of an object, such as converting a complex object to an image, the conversion must not introduce new metadata. The TOE can modify or add structural data, including fonts, without alerting the user if the modification is necessary for the proper display or print of the file.

### **Evaluation Activities** ▼

[\*FDP\\_NND\\_EXT.1\*](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure it describes the actions taken by the TOE when removing, simplifying, or redacting an element. If structural data is added, the TSS shall specify what structural data is added and the purpose of the structural data. If non-structural hidden data is added, the TSS shall detail the added hidden data and describe how the user is notified of the addition. The evaluator shall ensure that the TSS' description complies with the requirement to not introduce new hidden data, other than structural data, without warning the user.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create or acquire test files with complex objects or other elements and examine the files to locate those items in the structure. The examiner shall apply the TOE and examine the output to verify that no new hidden/metadata was introduced.*

## **FDP\_OBJ\_EXT.1 Removal of Objects and Corresponding References**

FDP\_OBJ\_EXT.1.1

The TOE must remove all references and indicators in the structural data to objects that are completely redacted by the TOE.

**Application Note:** In some formats, there are references in the structural data to objects, such as a name dictionary in PDF. If an object in a PDF document, such as an image, is completely redacted (i.e. the user has selected the entire image to be redacted), then not only must the image data be removed, but references to it in a name dictionary as well as all structural references to the image must be removed. If only part of the object is selected for redaction, then the references necessarily remain in the file since the object remains in the file.

## Evaluation Activities ▼

### [FDP\\_OBJ\\_EXT.1](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure its description of the removal of redacted objects includes the removal of all references and indicators to the redacted objects in conformance with the requirement.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create or acquire test files that contain objects and examine the files to locate these objects in the file format and all references to them in the structural data. The evaluator shall apply the TOE and select elements for complete redaction. The evaluator shall examine the output files to verify that the objects and all references to them have been redacted.*

## **FDP\_REM\_EXT.1 Removal of Redacted Data**

### FDP\_REM\_EXT.1.1

All data that is either selected by the user for redaction or identified by the TOE for redaction must be removed from the document.

**Application Note:** Selected content must be removed, not obscured by encryption, encoding, conversion to a proprietary format, or any other method.

## Evaluation Activities ▼

### [FDP\\_REM\\_EXT.1](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure it describes the removal of all data selected for redaction and verify that no encryption, encoding or proprietary process is used to obscure selected data. The evaluator shall ensure that the TSS' description complies with the requirement to remove all data selected by the user or identified by the TOE for redaction.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall acquire or create test files that contain text, images and other elements. The evaluator shall examine the test files to locate the content in the format. The evaluator shall apply the TOE, marking some of the content for redaction, and examine the output to verify that the marked content was removed and not obscured through encryption, encoding, or conversion to a proprietary format.*

## **FDP\_RIP\_EXT.1 Residual Information Removal**

### FDP\_RIP\_EXT.1.1

The TOE must automatically remove all remnant data, undo buffers, tracked changes buffers, multiple versions of the same object, and any buffer or cache type container of data.

**Application Note:** The user does not have to select this data for removal.

## Evaluation Activities ▼

### [FDP\\_RIP\\_EXT.1](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure it specifies the residual data and objects (e.g., remnant data, undo buffers, tracked changes buffers, multiple versions of the same object, and any buffer or cache type data container) that the TOE will remove from files without any user interaction. The evaluator shall ensure that the TSS' description complies with the requirement to automatically remove all such data.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**



*The evaluator shall create or acquire test files that contain the types of data described in the requirement and examine the files to locate the data. The evaluator shall apply the TOE and not select anything for redaction, and examine the files to verify that this data has been removed automatically.*

## **FDP\_RPL\_EXT.1 Visible Space Replace**

### **FDP\_RPL\_EXT.1.1**

The TOE must replace the visible space of redacted content in such a way that the visible space conveys no information about the previous contents.

**Application Note:** A vendor may use several different methods to replace content, such as opaque blocks, text, whitespace or some other vendor-defined method. These methods must not convey information about the content being replaced. For example, if text is replaced with text, the replacement text must not indicate length of component words. Blocks of color used to replace parts of images must not show variations in intensity that could convey information about the image content.

## **Evaluation Activities** ▼

### [\*FDP\\_RPL\\_EXT.1\*](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure it lists and describes the content used to replace redacted elements. The evaluator shall ensure that the TSS' description complies with the requirement to convey no information about the previous contents.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create or acquire a test file with an image, mark part of the image for redaction and apply the TOE, and examine the image in the output to verify that the visual appearance does not provide any indication of the content that was redacted. If the TOE allows text content to be replaced with text, the evaluator shall create or acquire a test file with some text as content, apply the TOE, and verify that the replacement text does not preserve word length or other identifying information that could allow recovery of the original content.*

## **FDP\_RVW\_EXT.1 Element Review**

### **FDP\_RVW\_EXT.1.1**

The TOE must allow the user to review and select each element of visible data in whole or in part for redaction.

**Application Note:** If the file or part of the file is encrypted, the TOE will have to reject the file or decrypt it so that the user can review the data.

## **Evaluation Activities** ▼

### [\*FDP\\_RVW\\_EXT.1\*](#)

#### **TSS**

*There are no TSS EAs for this component.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create test documents that contain images, text, and complex objects, apply the TOE and verify that each element is selectable for redaction in whole or in part.*

## **FDP\_SEL\_EXT.1 Selected Redaction**

### **FDP\_SEL\_EXT.1.1**

The TOE must [**selection:** *simplify, remove*] any complex object, embedded object or graphic image which is selected for redaction.

**Application Note:** The selection may be of either the whole element or only part of the element. If part of an element is selected, only that part must be

simplified or removed.

## Evaluation Activities ▼

### [FDP\\_SEL\\_EXT.1](#)

#### **TSS**

*The evaluator shall examine the TSS to ensure it describes in detail which complex objects can be simplified by the TOE and how they are simplified (e.g. whether the object or the whole page is converted to another format and what that format is). The TSS shall also list those complex objects or images that cannot be simplified and will be removed.*

#### **Guidance**

*There are no guidance EAs for this component.*

#### **Tests**

*The evaluator shall create or acquire test documents that contain complex objects and examine the documents to identify where those objects are in the format. The evaluator shall then apply the TOE and examine the output to verify that the objects have been simplified or removed. The evaluator shall test all objects that can be simplified as well as all objects that should be removed according to the TSS.*

*The evaluator shall also create or acquire test documents with complex objects that are not documented in the TSS, apply the TOE, and verify that those objects are removed from the document.*

## **FDP\_VAL\_EXT.1 Validation of Data**

### FDP\_VAL\_EXT.1.1

The TOE must remove unrecognized data, unexpected data, and extraneous structural data.

**Application Note:** Structural data is extraneous if it is unnecessary for the printing or display of the document contents, or unnecessary for the functionality of the document. Example - many formats include comments, e.g. PDF allows file format comments which are preceded by %. When these comments are unnecessary, unrelated to the printing or display of the content of the document, or provide no functionality whatsoever they must be removed.

Example - some formats expect a header structure starting at the first byte of a file, but a tool may be able to interpret a file where the header starts at a later byte by ignoring the data that precedes the header structure. In this case, the preceding data must be removed since it is unexpected.

### FDP\_VAL\_EXT.1.2

The TOE must [**selection:** *simplify, remove*] any element which it cannot completely interpret.

**Application Note:** For example, if the tool cannot recurse through a stream with embedded OLE objects, it must convert the stream to a single layer image with no metadata or remove it. If the redaction tool cannot interpret or process temporal objects, it must remove the temporal object and replace it with a simplified object or other placeholder. If a stream of data is compressed, encoded or encrypted and the redaction tool cannot uncompress, decode or decrypt the data, the tool must delete the stream.

## Evaluation Activities ▼

### [FDP\\_VAL\\_EXT.1](#)

#### **TSS**

*There are no TSS EAs for this element.*

*The evaluator shall examine the TSS to ensure that it describes how the TOE handles data that it cannot completely interpret.*

#### **Guidance**

*There are no guidance EAs for this element.*

*There are no guidance EAs for this element.*

#### **Tests**

*The evaluator shall create or acquire test files that contain unrecognized data, unexpected data, and extraneous structural data. The evaluator shall examine the files prior to redaction to*



*identify the data. The evaluator shall apply the TOE but make no visible redactions and save the output files. The evaluator shall examine the output files, comparing it to the originals, to verify that the data has been removed. The evaluator shall create or acquire test files with data that the TOE should not be able to completely interpret, apply the TOE and examine the output to verify that the TOE handled the data according to the requirement.*

### 5.0.3 Protection of the TSF (FPT)

#### FPT\_FLS.1 Failure with Preservation of Secure State

FPT\_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:  
[**assignment:** *list of types of failures in the TSF*].

**Application Note:** If the redaction functionality fails for any reason, the TOE must not produce a partially redacted file.

#### Evaluation Activities ▼

##### [FPT\\_FLS.1](#)

##### **TSS**

*The evaluator shall examine the TSS to ensure it describes what actions the TOE performs upon any failure. The evaluator shall ensure that the TSS' description complies with the requirement to not produce a partially redacted file.*

##### **Guidance**

*There are no guidance EAs for this component.*

##### **Tests**

*The evaluator shall create or acquire test files that cause the TOE to fail and observe that the TOE fails and does not produce partially redacted files.*

[CC] Common Criteria for Information Technology Security Evaluation -

- [Part 1: Introduction and General Model](#), CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
- [Part 2: Security Functional Components](#), CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- [Part 3: Security Assurance Components](#), CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.

[App PP] [Protection Profile for Application Software](#), Version 1.4, October 2021