PP-Module for Redaction Tools

Version: 1.1
2023-08-25
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2022-04-29	Initial publication
1.1	2023-08-25	Updates to conform to CC:2022

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
3.3 Organizational Security Policies
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
5.1 App PP Security Functional Requirements Direction
5.1.1 Modified SFRs
5.2 TOE Security Functional Requirements
5.2.1 Security Audit (FAU)
5.2.2 User Data Protection (FDP)
5.2.3 Security Management (FMT)
5.2.4 Protection of the TSF (FPT)
5.3 TOE Security Functional Requirements Rationale
6 Consistency Rationale
6.1 Protection Profile for Redaction Tools
6.1.1 Consistency of TOE Type
6.1.2 Consistency of Security Problem Definition
6.1.3 Consistency of Objectives
6.1.4 Consistency of Requirements
Appendix A - Optional SFRs
A.1 Strictly Optional Requirements
A.2 Objective Requirements
A.3 Implementation-based Requirements
Appendix B - Selection-based Requirements
Appendix C - Extended Component Definitions
C.1 Extended Components Table
C.2 Extended Component Definitions
C.2.1 Security Audit (FAU)
C.2.1.1 FAU_ALR_EXT Redaction Failure Notification
C.2.1.2 FAU_REP_EXT Report Generation
C.2.1.3 FAU_SAR_EXT Report Review
C.2.2 Security Management (FMT)
C.2.2.1 FMT_RVW_EXT Element Review
C.2.3 User Data Protection (FDP)
C.2.3.1 FDP_DID_EXT Identification of Data
C.2.3.2 FDP_DIN_EXT Deep Inspection
C.2.3.3 FDP_LOC_EXT Redact Content from Every Location
C.2.3.4 FDP_NND_EXT No New Data Introduced by TOE
C.2.3.5 FDP_OBJ_EXT Removal of Objects and Corresponding References
C.2.3.6 FDP_REM_EXT Removal of Redacted Data
C.2.3.7 FDP_RIP_EXT Residual Information Removal
C.2.3.8 FDP_RPL_EXT Visible Space Replace
C.2.3.9 FDP_SEL_EXT Selected Redaction
C.2.3.10 FDP_VAL_EXT Validation of Data
Appendix D - Acronyms
Appendix E - Bibliography

1 Introduction

1.1 Overview

The scope of the PP-Module for Redaction Tools, Version 1.1 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-PP:

- Protection Profile for Application Software, Version 2.0

This Base-PP is valid for this technology type because 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 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.

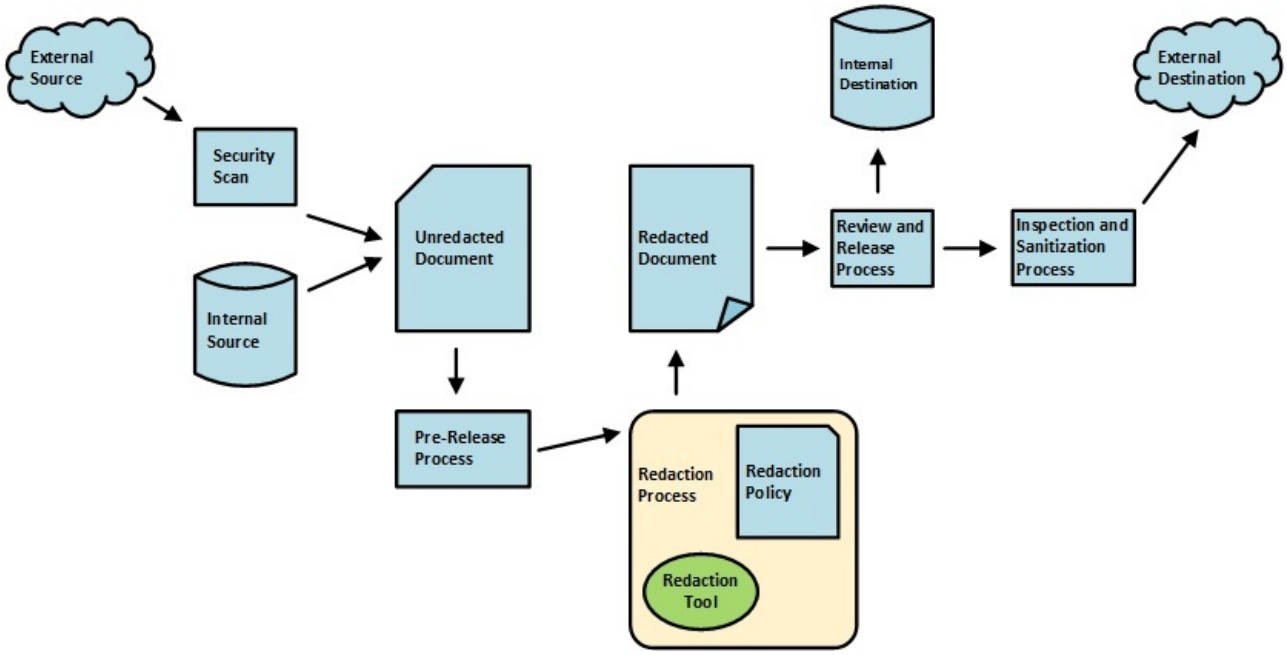


Figure 1: Sample Redaction Workflow

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, and 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	A Protection Profile developed by international technical communities and approved by multiple schemes.

Profile (cPP)	
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 Object Linking and Embedding (OLE) objects, Microsoft ActiveX controls, and temporal objects.
Functional	Forms, scripts, link URLs, workflow data, action buttons, formulas in a spreadsheet,

data	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, or portions of an embedded object (e.g., Microsoft 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, or 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 third-party apps, accessibility data such as alternate text, etc.
Steganography	The act of embedding covert data in an image file in such a way that the image alterations needed to embed the data are not readily visible to the naked eye.
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 visual representation of text, images, and complex objects in a file.

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/International Electrotechnical Commission (ISO/IEC)-29500 (Office Open XML, including but not limited to Microsoft Word, PowerPoint, and Excel documents), 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-Module 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; therefore, it 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 is 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

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs have sufficient supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1.

CC Conformance Claims

This PP is conformant to Parts 2 (extended) and 3 (extended) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any other Protection Profile.

No other PPs or PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module beyond its Base-PP.

Package Claim

- This PP-Module does not claim conformance to any functional packages.
- This PP-Module conforms to the EAL1 assurance package augmented with ALC_TSU_EXT.1, ASE_OBJ.2, ASE_REQ.2, and ASE_SPD.1.

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 add to the threats defined by the Base-PP.

T.CLUES_TO_ORIGINAL_DATA
A poorly-designed or poorly-implemented redaction tool can give false confidence of redaction by leaving clues to the nature of the original information in the redacted area of a document.

T.UNREDACTED_DATA
A poorly-designed or poorly-implemented redaction tool can give false confidence of redcation by failing to remove user-selected visible or hidden data in such a way that the original information is inadvertently distributed.

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 about 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 such as resolving and disabling tracked changes prior to redaction, working with a copy of the document to preserve the original file, and removing passwords and decrypting files.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

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

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. These metadata and elements include, but are 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 or is located in the header and footer sections of the file.

O.PROPER_OUTPUT
The TOE will react to unexpected input data or behavior by ensuring that it will not produce an output document with insufficient redactions made or with its own additions made.

O.REDACTION
The TOE will provide the ability to completely remove any data selected for redaction.

O.REPORT
The TOE will provide the ability to produce a report of all data that was redacted and any errors that occurred during redaction.

O.REVIEW
The TOE will provide the ability for a user to review a document to select the data that will be redacted in it.

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.KNOWLEDGEABLE_USER
The organization takes steps to ensure that users entrusted to operate the TOE have adequate training in its use and in related document management activities.

OE.INFORMATION_RELEASE_POLICY
The organization develops an information release policy that is clearly communicated to TOE users so that users have sufficient information to apply correct redactions.

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.INSPECTION	The TOE mitigates the threat of clues to unredacted data by ensuring that the entire document is searched for redactable information, including hidden data and metadata.
	O.REDACTION	The TOE mitigates the threat of clues to unredacted data by ensuring that the redaction process replaces the visible space of redacted data in a way that leaves no clues as to the original unredacted data.
T.UNREDACTED_DATA	O.PROPER_OUTPUT	The TOE mitigates the threat of unredacted data by ensuring that unexpected or corrupted inputs do not cause the TOE to fail in a way that would generate an unredacted or improperly redacted output.
	O.REDACTION	The TOE mitigates the threat of unredacted data by implementing a redaction function.
	O.REPORT	The TOE mitigates the threat of unredacted data by generating a report that clearly shows to the user what

		data was redacted.
	O.REVIEW	The TOE mitigates the threat of unredacted data by allowing the user to specify the data that will be redacted from a document.
A.KNOWLEDGEABLE_USER	OE.KNOWLEDGEABLE_USER	The assumption is realized through achievement of an organizational objective that accomplishes the goal of the assumption.
P.INFORMATION_RELEASE_POLICY	OE.INFORMATION_RELEASE_POLICY	The assumption is realized through achievement of an organizational objective that accomplishes the goal of the assumption.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 App PP Security Functional Requirements Direction

In a PP-Configuration that includes the App PP, there are no App PP requirements that must be claimed in a certain manner for redaction functionality to be correctly implemented. Therefore, all SFR operations may be performed at the ST author's discretion.

5.1.1 Modified SFRs

This PP-Module does not modify any SFRs defined by the App PP.

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 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.

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.

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.

5.2.2 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_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 redaction operation 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 data or 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_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.

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 printing of the file.

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), any references to the image in a name dictionary or structural references to the image must also 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.

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.

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 data container.

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

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.

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 that 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.

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. For example, many formats include comments, such as the PDF format which uses a percent sign (%) to precede file format comments.

When these comments are unnecessary, are unrelated to the printing or display of the content of the document, or do not provide any functionality, they must be removed.

For 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 decompress, decode, or decrypt the data, the tool must delete the stream.

5.2.3 Security Management (FMT)

FMT_RVW_EXT.1 Element Review

FMT_RVW_EXT.1.1

The TSF shall identify the visible data elements that the user can select 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.

5.2.4 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.

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 2: SFR Rationale

Objective	Addressed by	Rationale
O.INSPECTION	FDP_DID_EXT.1	This requirement supports the objective by requiring the TOE to implement a mechanism to inspect a document for common mechanisms used to hide unredacted data.
	FDP_DIN_EXT.1	This requirement supports the objective by defining a deep inspection mechanism by which the TOE can examine hidden data or metadata to find unredacted data.
O.PROPER_OUTPUT	FDP_NND_EXT.1	This requirement supports the objective by prohibiting the TOE from introducing new data to a file without the user's instruction.
	FDP_VAL_EXT.1	This requirement supports the objective by requiring the TOE to implement a mechanism that allows it to handle unrecognizable data.
	FPT_FLS.1	This requirement supports the objective by requiring the TOE to maintain a secure state (i.e., do not produce unvalidated and potentially unredacted output) if it encounters a failure or some other unexpected event.
O.REDACTION	FDP_LOC_EXT.1	This requirement supports the objective by requiring the TOE to remove redacted content from every location in the source file.
	FDP_OBJ_EXT.1	This requirement supports the objective by requiring the TOE to remove references to redacted data in the source file.
	FDP_REM_EXT.1	This requirement supports the objective by requiring the TOE to redact all data that has been selected for redaction.
	FDP_RIP_EXT.1	This requirement supports the objective by requiring the TOE to purge all residual data so that unredacted data cannot be extracted from memory.
	FDP_RPL_EXT.1	This requirement supports the objective by requiring the TOE to replace the visible space of redacted documents in a manner that does not provide clues to the original unredacted data.
	FDP_SEL_EXT.1	This requirement supports the objective by defining how the TOE handles complex objects that are selected for redaction, whether by simplification or removal.
O.REPORT	FAU_ALR_EXT.1	This requirement supports the objective by requiring the TOE to notify the user of unsuccessful redaction operations.
	FAU_REP_EXT.1	This requirement supports the objective by identifying the contents of any report that the TOE generates about its redaction behavior.
	FAU_SAR_EXT.1	This requirement supports the objective by requiring the TOE allow the user to access reports on redacted data.
O.REVIEW	FMT_RVW_EXT.1	This SFR supports the objective by defining the requirement to review and select data to be redacted.

6 Consistency Rationale

6.1 Protection Profile for Redaction Tools

6.1.1 Consistency of TOE Type

If 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 the redaction tool functionality that is built into the application so that additional security functionality is claimed within the scope of the TOE.

The only asset for the TOE is the software executable and sensitive data that comprises the TOE. The entire TOE as defined by the combination of the Base-PP and this PP-Module is a single asset. The only differences to the threat model are that the PP-Module introduces threats related specifically to the failure of the TOE to fully redact data, which is a use case specific to redaction tools.

6.1.2 Consistency of Security Problem Definition

Listed below are the threats, objectives, and OSPs defined in this PP-Module with rationale for their consistency with the App PP. The PP-Module shares the executable application asset with the App PP but defines additional threats because the PP-Module defines a specific type of software application with potential exploits that are common to the application type.

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.CLUES_TO_ORIGINAL_DATA	This threat is consistent with the Base-PP because it relates to functionality that is exclusive to the PP-Module.
T.UNREDACTED_DATA	This threat is consistent with the Base-PP because it relates to functionality that is exclusive to the PP-Module.
A.KNOWLEDGEABLE_USER	This assumption is an extension of the A.PROPER_USER and A.PROPER_ADMIN assumptions in the Base-PP but extends them to apply specifically to the operation of redaction tools.
P.INFORMATION_RELEASE_POLICY	The Base-PP does not define any organizational security policies so there are no existing policies that this could contradict.

6.1.3 Consistency of Objectives

Listed below are the security objectives defined in this PP-Module with rationale for their consistency with the App PP. The PP-Module shares the executable application asset with the App PP but defines additional security objectives because the PP-Module defines a specific type of software application with security functionality that is common to the application type. The objectives for the TOEs are consistent with the App PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.INSPECTION	This objective relates solely to redaction behavior, which is beyond the scope of the Base-PP and does not prevent any Base-PP objectives from being satisfied.
O.PROPER_OUTPUT	This objective relates solely to redaction behavior, which is beyond the scope of the Base-PP and does not prevent any Base-PP objectives from being satisfied.
O.REDACTION	This objective relates solely to redaction behavior, which is beyond the scope of the Base-PP and does not prevent any Base-PP objectives from being satisfied.
O.REPORT	This objective relates solely to redaction behavior, which is beyond the scope of the Base-PP and does not prevent any Base-PP objectives from being satisfied.
O.REVIEW	This objective relates solely to redaction behavior, which is beyond the scope of the Base-PP and does not prevent any Base-PP objectives from being satisfied.

The objectives for the TOE's OE are consistent with the App PP based on the following rationale:

PP-Module OE Objective	Consistency Rationale
OE.KNOWLEDGEABLE_USER	This objective is an extension of the OE.PROPER_USER and OE.PROPER_ADMIN objectives in the Base-PP but extends them to apply specifically to the operation of redaction tools.
OE.INFORMATION_RELEASE_POLICY	This objective does not contradict the Base-PP because it describes the implementation of an organizational security policy.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the App PP that are needed to support Redaction Tool functionality. This is considered to be consistent because the functionality provided by the App PP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the App PP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
This PP-Module does not modify any requirements when the App PP is the base.	
Additional SFRs	
This PP-Module does not add any requirements when the App PP is the base.	
Mandatory SFRs	
FAU_ALR_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FAU_REP_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FAU_SAR_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_DID_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_DIN_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_LOC_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_NND_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_OBJ_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_REM_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_RIP_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_RPL_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_SEL_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FDP_VAL_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FMT_RVW_EXT.1	This requirement relates to redaction functionality, which is beyond the scope of the Base-PP and does not prevent any Base-PP requirements from being implemented.
FPT_FLS.1	This requirement relates to the preservation of a secure state in the event of a TSF failure. This is not defined in the Base-PP but the Base-PP has no requirements that prohibit it.
Optional SFRs	
This PP-Module does not define any Optional requirements.	
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-based SFRs	
This PP-Module does not define any Implementation-based requirements.	

Selection-based SFRs

This PP-Module does not define any Selection-based requirements.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

This PP-Module does not define any Strictly Optional SFRs.

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-based Requirements

This PP-Module does not define any Implementation-based SFRs.

Appendix B - Selection-based Requirements

This PP-Module does not define any Selection-based SFRs.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 3: Extended Component Definitions

Functional Class	Functional Components
Security Audit (FAU)	FAU_ALR_EXT Redaction Failure Notification FAU_REP_EXT Report Generation FAU_SAR_EXT Report Review
Security Management (FMT)	FMT_RVW_EXT Element Review
User Data Protection (FDP)	FDP_DID_EXT Identification of Data FDP_DIN_EXT Deep Inspection FDP_LOC_EXT Redact Content from Every Location FDP_NND_EXT No New Data Introduced by TOE FDP_OBJ_EXT Removal of Objects and Corresponding References FDP_REM_EXT Removal of Redacted Data FDP_RIP_EXT Residual Information Removal FDP_RPL_EXT Visible Space Replace FDP_SEL_EXT Selected Redaction FDP_VAL_EXT Validation of Data

C.2 Extended Component Definitions

C.2.1 Security Audit (FAU)

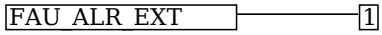
This PP-Module defines the following extended components as part of the FAU class originally defined by CC Part 2:

C.2.1.1 FAU_ALR_EXT Redaction Failure Notification

Family Behavior

Components in this family describe requirements for user notification in response to a specific kind of TSF failure.

Component Leveling



FAU_ALR_EXT.1, Redaction Failure Notification, requires the TSF to generate a notification in the event of a failed redaction operation.

Management: FAU_ALR_EXT.1

There are no management activities foreseen.

Audit: FAU_ALR_EXT.1

There are no auditable events foreseen.

FAU_ALR_EXT.1 Redaction Failure Notification

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FPT_FLS.1 Failure with Preservation of Secure State

FAU_ALR_EXT.1.1

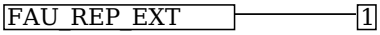
The TOE must make the user aware when redaction fails for any reason.

C.2.1.2 FAU_REP_EXT Report Generation

Family Behavior

Components in this family define requirements for the generation of report data in response to a specific TSF action being performed.

Component Leveling



FAU_REP_EXT.1, Report Generation, requires the TSF to generate a report following the completion of a redaction operation that identifies the elements that were redacted along with metadata about each redaction.

Management: FAU_REP_EXT.1

There are no management activities foreseen.

Audit: FAU_REP_EXT.1

There are no auditable events foreseen.

FAU_REP_EXT.1 Report Generation

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FAU_REP_EXT.1.1

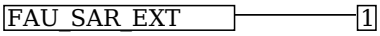
The TOE must be able to generate a report entry that contains metadata about each element that was redacted, including at least the following: the type of the element that was removed, the location if it was a visible element, and whether the element was selected by the user or removed automatically.

C.2.1.3 FAU_SAR_EXT Report Review

Family Behavior

Components in this family define requirements for user review of a specific type of TSF data.

Component Leveling



FAU_SAR_EXT.1, Report Review, requires the TSF to have its generated report data be user-reviewable.

Management: FAU_SAR_EXT.1

The following actions could be considered for the management functions in FMT:

- View contents of generated report

Audit: FAU_SAR_EXT.1

There are no auditable events foreseen.

FAU_SAR_EXT.1 Report Review

Hierarchical to: No other components.

Dependencies to: FAU_REP_EXT.1 Report Generation

FAU_SAR_EXT.1.1

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

C.2.2 Security Management (FMT)

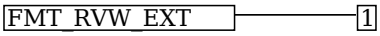
This PP-Module defines the following extended components as part of the FMT class originally defined by CC Part 2:

C.2.2.1 FMT_RVW_EXT Element Review

Family Behavior

Components in this family define functionality for selecting data elements that can be redacted from a document.

Component Leveling



FMT_RVW_EXT.1, Element Review, requires the TSF to present a user interface that can be used to select data elements for redaction.

Management: FMT_RVW_EXT.1

The following actions could be considered for the management functions in FMT:

- Selection of data elements to be redacted

Audit: FMT_RVW_EXT.1

There are no auditable events foreseen.

FMT_RVW_EXT.1 Element Review

Hierarchical to: No other components.

Dependencies to: No dependencies.

FMT_RVW_EXT.1.1

The TSF shall identify the visible data elements that the user can select in whole or in part for redaction.

C.2.3 User Data Protection (FDP)

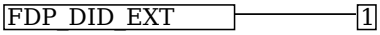
This PP-Module defines the following extended components as part of the FDP class originally defined by CC Part 2:

C.2.3.1 FDP_DID_EXT Identification of Data

Family Behavior

Components in this family define requirements for the identification of data within a document that can be considered for redaction.

Component Leveling



FDP_DID_EXT.1, Identification of Data, requires the TSF to identify all hidden or obscured data in a document so that this data can be selectable for redaction.

Management: FDP_DID_EXT.1

The following actions could be considered for the management functions in FMT:

- Specify how the redaction operation is applied to small or low-resolution image data

Audit: FDP_DID_EXT.1

There are no auditable events foreseen.

FDP_DID_EXT.1 Identification of Data

Hierarchical to: No other components.

Dependencies to: FMT_RVW_EXT.1 Element Review

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.

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*].

FDP_DID_EXT.1.3

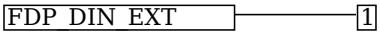
The TOE must identify images where the visible representation is reduced in size or resolution from the representation stored in the file format and must [**selection**: *automatically replace the stored data with the visible representation, allow the user to replace the stored data with the visible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

C.2.3.2 FDP_DIN_EXT Deep Inspection

Family Behavior

Components in this family define requirements for inspecting document metadata for potential redaction.

Component Leveling



FDP_DIN_EXT.1, Deep Inspection, requires the TSF to handle redaction of file metadata in a specified manner.

Management: FDP_DIN_EXT.1

There are no management activities foreseen.

Audit: FDP_DIN_EXT.1

There are no auditable events foreseen.

FDP_DIN_EXT.1 Deep Inspection

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_DIN_EXT.1.1

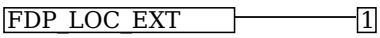
For each element of the file format that can contain its own metadata, other elements, or hidden data, the TOE must [**selection**: *recurse through the element chain and apply the redaction operation to each layer, simplify the element, redact the element*].

C.2.3.3 FDP_LOC_EXT Redact Content from Every Location

Family Behavior

Components in this family define requirements for the thoroughness of a data redaction process.

Component Leveling



FDP_LOC_EXT.1, Redact Content from Every Location, requires the TSF to have the ability to redact data from all possible locations in an input file.

Management: FDP_LOC_EXT.1

There are no management activities foreseen.

Audit: FDP_LOC_EXT.1

There are no auditable events foreseen.

FDP_LOC_EXT.1 Redact Content from Every Location

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_LOC_EXT.1.1

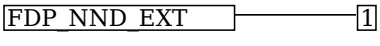
The TOE must remove redacted content from every location in the file format where it is stored.

C.2.3.4 FDP_NND_EXT No New Data Introduced by TOE

Family Behavior

Components in this family apply restrictions on data that the TOE can add to a file as part of the redaction process.

Component Leveling



FDP_NND_EXT.1, No New Data Introduced by TOE, requires the TSF to avoid the introduction of its own

data to an input file unless explicitly requested by a user.

Management: FDP_NND_EXT.1

The following actions could be considered for the management functions in FMT:

- Specification or approval of introduced hidden data

Audit: FDP_NND_EXT.1

There are no auditable events foreseen.

FDP_NND_EXT.1 No New Data Introduced by TOE

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_NND_EXT.1.1

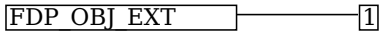
The TOE itself must not introduce new hidden data that was not requested by the user without warning the user of the addition.

C.2.3.5 FDP_OBJ_EXT Removal of Objects and Corresponding References

Family Behavior

Components in this family define requirements for the removal of object references as part of a data redaction process.

Component Leveling



FDP_OBJ_EXT.1, Removal of Objects and Corresponding References, requires the TSF to remove references to redacted objects so as not to disclose information about the data that was redacted.

Management: FDP_OBJ_EXT.1

There are no management activities foreseen.

Audit: FDP_OBJ_EXT.1

There are no auditable events foreseen.

FDP_OBJ_EXT.1 Removal of Objects and Corresponding References

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_OBJ_EXT.1.1

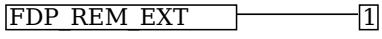
The TOE must remove all references and indicators in the structural data to objects that are completely redacted by the TOE.

C.2.3.6 FDP_REM_EXT Removal of Redacted Data

Family Behavior

Components in this family define requirements for the application of a redaction operation to selected data.

Component Leveling



FDP_REM_EXT.1, Removal of Redacted Data, requires the TSF to redact all selected data.

Management: FDP_REM_EXT.1

There are no management activities foreseen.

Audit: FDP_REM_EXT.1

There are no auditable events foreseen.

FDP_REM_EXT.1 Removal of Redacted Data

Hierarchical to: No other components.

Dependencies to: FMT_RVW_EXT.1 Element Review

FDP_REM_EXT.1.1

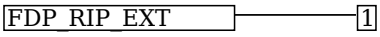
All data that is either selected by the user for redaction or identified by the TOE for redaction must be removed from the document.

C.2.3.7 FDP_RIP_EXT Residual Information Removal

Family Behavior

Components in this family define requirements for the purging of residual data that could compromise the effectiveness of a redaction operation.

Component Leveling



FDP_RIP_EXT.1, Residual Information Removal, requires the TSF to delete all residual file data that could contain unredacted information.

Management: FDP_RIP_EXT.1

There are no management activities foreseen.

Audit: FDP_RIP_EXT.1

There are no auditable events foreseen.

FDP_RIP_EXT.1 Residual Information Removal

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_RIP_EXT.1.1

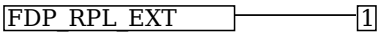
The TOE must automatically remove all remnant data, undo buffers, tracked changes buffers, multiple versions of the same object, and any buffer or cache type data container.

C.2.3.8 FDP_RPL_EXT Visible Space Replace

Family Behavior

Components in this family define requirements for the visual presentation of redacted data.

Component Leveling



FDP_RPL_EXT.1, Visible Space Replace, requires the TSF to replace redacted data with visual data that does not give clues as to the contents of the original data.

Management: FDP_RPL_EXT.1

There are no management activities foreseen.

Audit: FDP_RPL_EXT.1

There are no auditable events foreseen.

FDP_RPL_EXT.1 Visible Space Replace

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_RPL_EXT.1.1

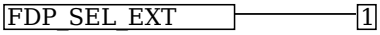
The TOE must replace the visible space of redacted content in such a way that the visible space conveys no information about the previous contents.

C.2.3.9 FDP_SEL_EXT Selected Redaction

Family Behavior

Components in this family define requirements for the selection of redacted data.

Component Leveling



FDP_SEL_EXT.1, Selected Redaction, requires the TSF to redact data from complex objects in a specified manner.

Management: FDP_SEL_EXT.1

There are no management activities foreseen.

Audit: FDP_SEL_EXT.1

There are no auditable events foreseen.

FDP_SEL_EXT.1 Selected Redaction

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_SEL_EXT.1.1

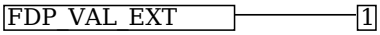
The TOE must [**selection**: *simplify*, *remove*] any complex object, embedded object, or graphic image that is selected for redaction.

C.2.3.10 FDP_VAL_EXT Validation of Data

Family Behavior

Components in this family define requirements for validating data as part of its consideration for redaction.

Component Leveling



FDP_VAL_EXT.1, Validation of Data, requires the TOE to remove unexpected or other file data that cannot be validated.

Management: FDP_VAL_EXT.1

There are no management activities foreseen.

Audit: FDP_VAL_EXT.1

There are no auditable events foreseen.

FDP_VAL_EXT.1 Validation of Data

Hierarchical to: No other components.

Dependencies to: FDP_REM_EXT.1 Removal of Redacted Data

FDP_VAL_EXT.1.1

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

FDP_VAL_EXT.1.2

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

Appendix D - Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
EP	Extended Package
EXIF	Exchangeable Image File Format
FP	Functional Package
ISO/IEC	International Standards Organization/International Electrotechnical Commission
JPG	Joint Photographic Experts Group
OE	Operational Environment
OLE	Object Linking and Embedding
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TIFF	Tagged Image File Format
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

Appendix E - Bibliography

Identifier	Title
[App PP]	Protection Profile for Application Software, Version 2.0, TBD
[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.
[CEM]	Common Methodology for Information Technology Security - Evaluation Methodology, CCMB-2022-11-006, CEM:2022, Revision 1, November 2022.