

General Data Protection Regulation (GDPR) Statement McAfee Hardware Returns

McAfee Manufacturing

Last updated: May 3, 2018

GDPR Process Statement version 1.0

Contents

- ▶ [Scope](#)
- ▶ [Hardware returns process](#)
- ▶ [Full box replacement procedure](#)
- ▶ [Parts replacement onsite procedure](#)
- ▶ [HP Blade Servers](#)
- ▶ [PII Data captured or processed](#)
- ▶ [Data transfer](#)
- ▶ [Data security](#)
- ▶ [Data retention](#)
- ▶ [Identification](#)
- ▶ [Appendix 1](#)
- ▶ [Appendix 2](#)
- ▶ [Appendix 3](#)
- ▶ [Appendix 4](#)
- ▶ [Appendix 5](#)

Scope

This document covers the general procedures in place for hardware returns for McAfee Corporate Products which include:

- McAfee Email Gateway
- McAfee Web Gateway
- McAfee Data Loss Prevention (DLP)
- McAfee Enterprise Security Manager (SIEM)
- McAfee Network Security Platform (IPS)
- McAfee Advanced Threat Defense (ATD)

In general, customer hardware returns requests can be categorized either as:

- **Full box replacement**
- **Parts replacement on site.**

See the McAfee Hardware Support User Guide for hardware support programs. (Link located in Appendix 4.)

Hardware returns process

McAfee Support begins diagnosing when the customer raises a hardware issue. Reference to the standard support operating and diagnostic procedures can be found here¹.

Note: Full Box and Parts replacement components are transported in a secure way with tracking by a top tier third party courier company.

Appendix 1 shows the McAfee Hardware Returns process.

Full box replacement procedure

McAfee Support triggers a Support RMA request when a full box replacement decision is given to the customer. The customer is sent a full box replacement unit to replace the faulty unit and are given details about returning the faulty unit.

When the full box replacement request is received² from a customer, use the following procedure:

Procedure	Notes
1. Manufacturing received the returned unit, HDD/SSD to be removed.	All units returned from the field due to a technical failure must have failure analysis, except for the products based on legacy platform*.
2. HDD/SSD to be checked for its recycle value and then either: a. Scrapped /destroyed b. Wiped securely before the unit gets tested.	HDD/SSD to be reviewed whether to reuse or scrap. The review process is documented in ETN.
3. Returned unit to be going through McAfee production testing including failure analysis test. a. HDD/SSD to be sanitized before being tested.	HDD/SSD is failure analysis tested and is wiped clean and does not contain any PII data after being sanitized.
4. If the identified parts are repairable : a. Contract manufacture will get the unit fixed and reset to factory default settings. b. The unit will go into ETN inventory as replacement unit for next customer.	See ETN

¹ See Appendix 5 [McAfee Hardware Support Handbook](#)

² See Appendix 4 for the Support returns process flow

<p>5. If the part is identified as scrapable, the following process takes place:</p> <ol style="list-style-type: none"> a. Request to scrap received from McAfee b. Contract manufacture issues order to deplete requested parts and quantities from inventory c. Parts picked and placed into scrap/QX area d. E-waste contractor contacted for quote e. Quote provided to McAfee for approval f. Quote approved, E-waste vendor picks up material and processes as e-waste g. Certificate of Destruction provided after completion of e-waste process 	<p>See SCRAP</p>
---	------------------

*Notes: McAfee Equivalent to New (ETN) process INST-0581-00, governs the decision for disposition of appliances and control actions to be carried out by McAfee Manufacturing Partner.

ETN (Equivalent To New)

McAfee Manufacturing Partner follows ETN procedure (INST-0581-00 rev. Q) to make proper decisions for the disposition of appliances and materials that come from this process. See the document instructions (section 7, ETN Instructions).

- INST-0581-00.
- Delete Customer Data on working HDD and SSDs, "Shred".

Scrap

When hardware is set to be scrapped, the following procedure must be followed:

- INST-0581-00, ETN instruction (Sec. 7.1.3.3)
- Once determined to be scrapped, the vendor collects the units using the secure collection protocol. Certificate of Destruction is given to CONTRACT MANUFACTURE.

Procedure	Notes
1. McAfee Manufacturing to raise a scrap FG request.	FG request raised.
2. McAfee manufacturing partner: <ol style="list-style-type: none"> a. To consolidate/verify scrap list. b. To verify if any HDD/SSD included in appliance. 	Scrap list prepared ³ .
3. HDD/SSD found in appliance: <ol style="list-style-type: none"> a. HDD/SSD to be formatted/wiped with hddclean.sh tool on bootable unit. b. HDD/SSD is destroyed with a hammer or by drilling holes in it. 	HDD/SSD is wiped clean and destroyed. The unit does not contain any PII data after being sanitized.
4. The appliance to be shipped to E-waste company and the physical parts are destroyed.	

Appendix 2 shows the scrap process carried out by Contract Manufacture.

³ McAfee scrap record with certificate of destruction TCG ref

When raw material being scrapped, the following procedure must be followed:

Procedure	Notes
1. McAfee Manufacturing to raise a scrap request.	
2. McAfee manufacturing partner: <ul style="list-style-type: none"> a. To consolidate/verify scrap list. b. To carry out system process. 	<ul style="list-style-type: none"> a. Request to scrap received from McAfee b. Contract manufacture issues order to deplete requested parts and quantities from inventory c. Parts picked and placed into scrap/QX area d. E-waste contractor contacted for quote e. Quote provided to McAfee for approval f. Quote approved, E-waste vendor picks up material and processes as e-waste g. Certificate of destruction provided after completion of e-waste process
3. The appliance to be shipped to E-waste company and physical parts are destroyed.	

When component taken from returned RMA hardware is set to the scrapped, the following procedure must be followed:

Procedure	Notes
1. Verify HDD/SSD is taken from original RMA appliance.	
2. Format/Wipe HDD/SSD with hddclean.sh tool on bootable unit.	HDD/SSD is wiped clean and will not contain any PII data.
3. Check if HDD/SSD is in the warranty period: <ul style="list-style-type: none"> a. Yes, in warranty: <ul style="list-style-type: none"> i. Process HDD/SSD for RTV. ii. Notify McAfee manufacturing partner to receive replacement part. b. No: <ul style="list-style-type: none"> i. HDD/SSD is destroyed with hammer or by drilling holes in it. ii. Put destroyed HDD/SSD to be put in defective location and wait for McAfee scrap instruction. 	<p>HDD/SSD processed for RTV.</p> <p>McAfee manufacturing partner notified to receive replacement part.</p> <p>HDD/SSD is destroyed, to be collected for scrap.</p>

Sample of Scrap process details can be found in McAfee Manufacturing Partners documents⁴.

Parts replacement onsite procedure

Replacement part is sent to customer when parts replacement onsite decision is made, based on the part and the customer service level.

Onsite part replacement installation is carried out either by:

⁴ TCG Recycling Process Overview, NCR - Zenzar Disk Drive Testing and Erasure Process.

- Customer themselves or
- An authorized service technician/partner.

Note: It is no longer compulsory for customers to return HDD/SSD⁵.

McAfee authorized service technician/partner

When an authorized service technician/partner visiting customer onsite, the following procedure for parts replacement onsite must be followed:

1. Contact customer to ensure part received onsite, arrange a suitable appointment.
2. Examine and verify component received by customer.
3. Update customer record of the new component part.
4. Remove the fault part from customer equipment.
5. Replace it with the new component part.
6. Verify the replaced part is in a good and functioning condition.
7. Encourage customer to destroy HDD/SSD or retain the part.
 - a. Customer decided to destroy / keep part themselves (Certificate of Destruction/Media Retention Statement)
 - b. Customer decides to return the part:
 - i. A single page document attached to all HDD/SSD boxes provides return instructions.
 - ii. Customer contacts OnProcess technology and is provided a return waybill kit for Choice location in Netherlands (all EU locations) or Choice location in Dallas, TX (all other locations).
 - iii. Customer returns the part to the Choice depot where it is scrapped and a certificate of destruction is provided.

Customer

When customers have chosen to have replacement parts delivered onsite and replace them themselves, the following procedure for parts replacement must be followed:

1. The correct part for replacement is sent to customer securely via an authorized courier.
2. Customer accepts and verifies that the part received is correct.
3. Customer carries out part replacement installation and accepts the quality of HDD/SSD.
4. Customer to decide⁶:
 - a. To retain faulty part and dispose faulty part themselves by issuing McAfee:
 - i. Certificate of Destruction (COD) – part is destroyed by customer.
 - ii. Media Retention Statement (MRS) – part is retained by customer.
 - b. Customer decides to return the part:
 - i. Return instructions for all HDD/SSD are included in the box.

⁵ Customers are encouraged to destroy HDD/SSD themselves.

⁶ Note The customer may be contacted by OnProcess⁶, an expediting service provider that McAfee use to encourage customer to return the fault parts.

- ii. Customer contacts On Process technology and is provided a return waybill kit for Choice location in Netherlands (all EU locations) or Choice location in Dallas, TX (all other locations).
- iii. Customer returns the part to the Choice depot where it is scrapped and a certificate of destruction is provided.

See your hardware support level agreement for range of components considered to be parts that are covered by this Parts replacement onsite section.

HP Blade Servers

Our authorized service partner (NCR) handles all HP Blade Server returns. NCR directs the case to Zenzar, a company that owns HP Blade Servers material.

Note McAfee Manufacturing does not handle returned blades and Zenzar has its own process to wipe clean data⁷.

PII Data captured or processed

McAfee Manufacturing does not capture any PII data for hardware return.

See Full box replacement procedure (pg. 4) and Parts replacement onsite procedure (pg. 8) for further detail.

Data transfer

All transfer for hardware return for both full box replacement and parts replacement onsite processed securely by our authorized service partner.

Data security

McAfee Manufacturing as well as our authorized service partner have access control policy to ensure returned unit including HDD/SSD are stored securely in access control area.

Data retention

McAfee Manufacturing as well as our authorized service partner do not retain PII data. Returned unit including HDD/SSD is processed (wipe clean or destroyed) in a reasonable time (up to 10 business working days on receipt of equipment).

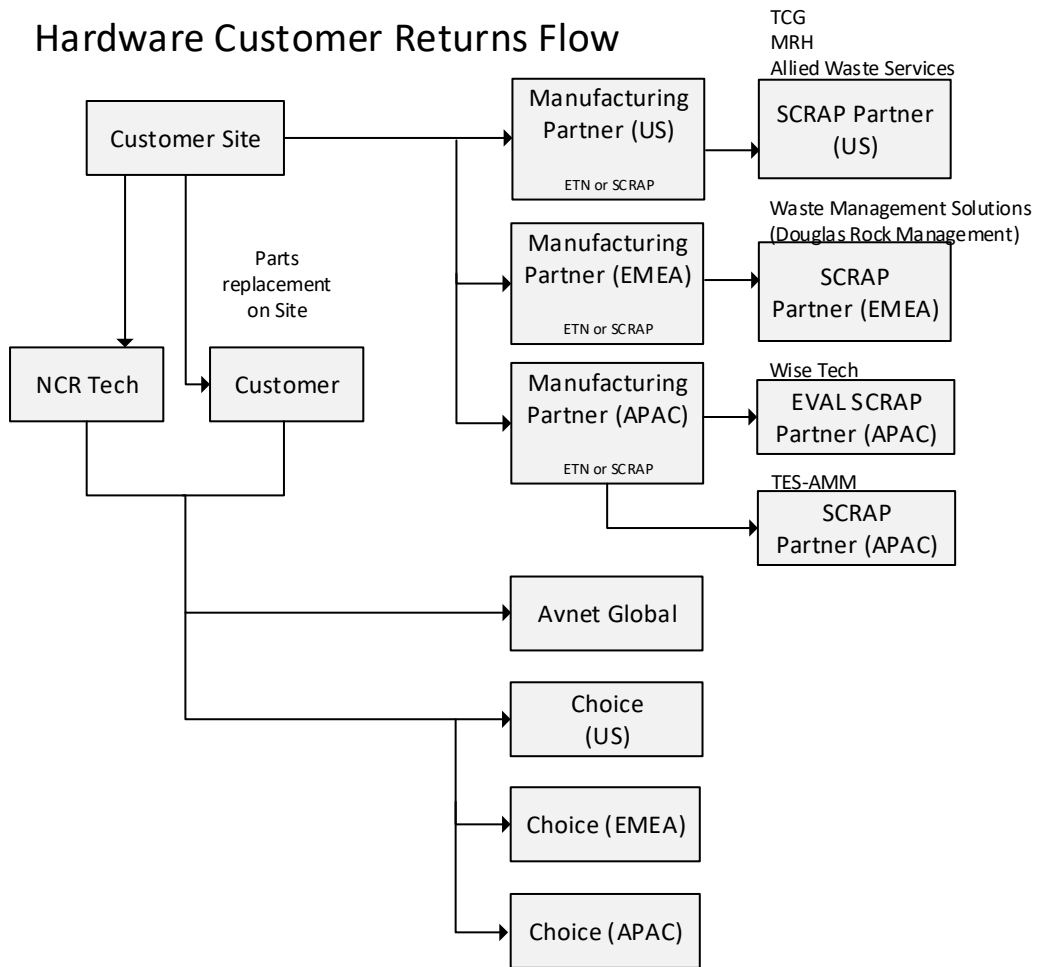
Identification

McAfee Manufacturing perform periodically process as well as contract review with our authorized partners to ensure GDPR compliance.

⁷ NCR - Zenzar Disk Drive Testing and Erasure Process.

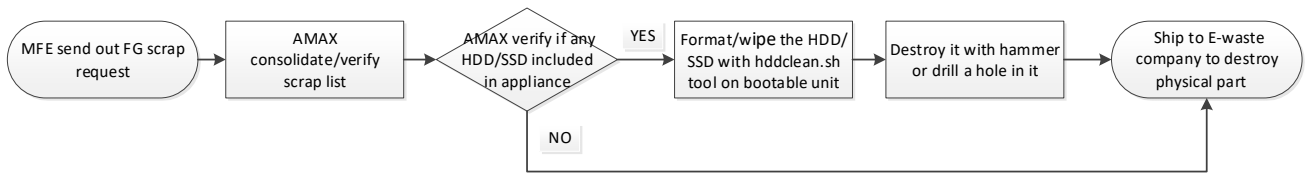
Appendix 1

Hardware Customer Returns Flow



Appendix 2

Scrap process - AMAX China



Raw material scrap

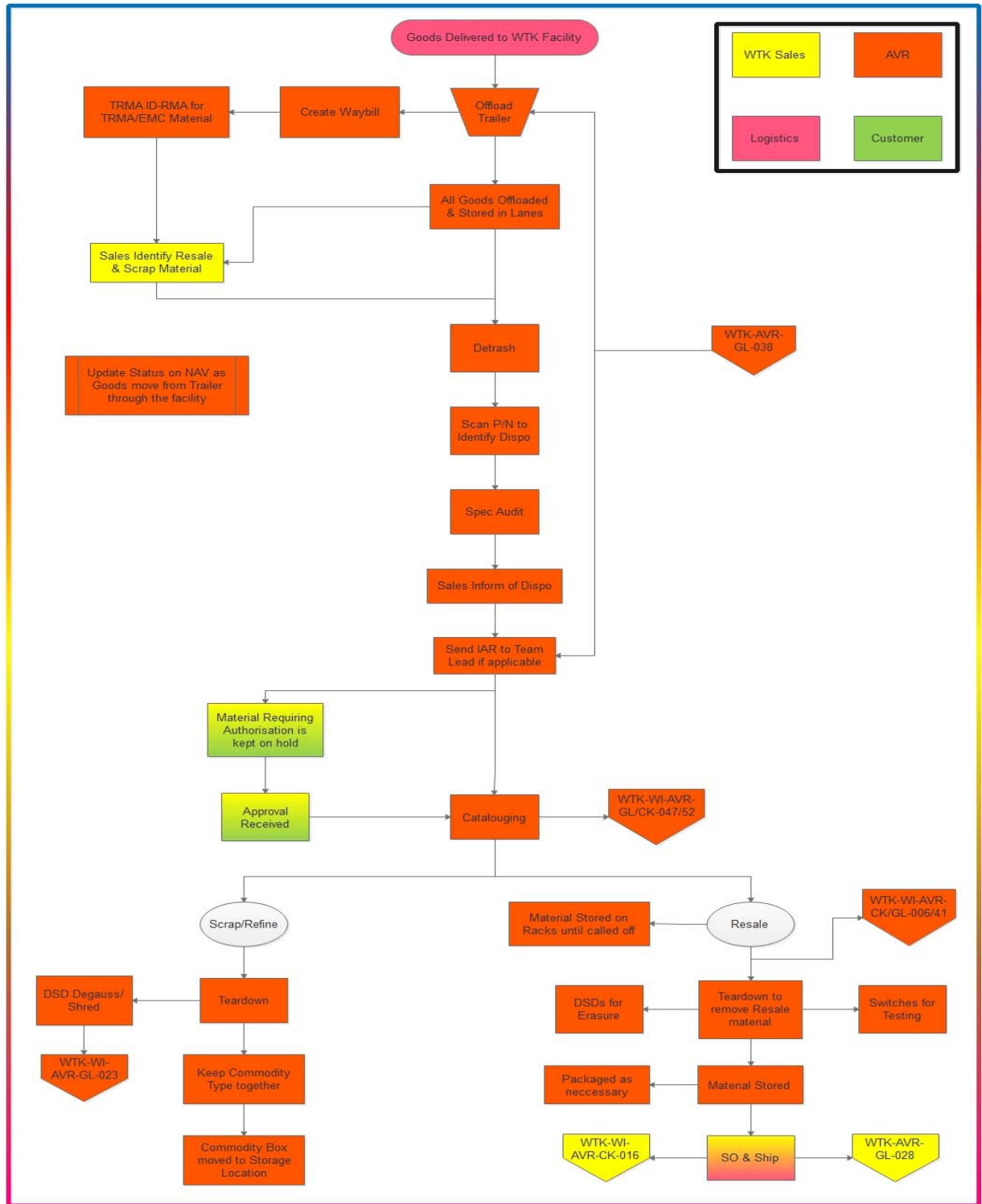


Component taken from returned RMA

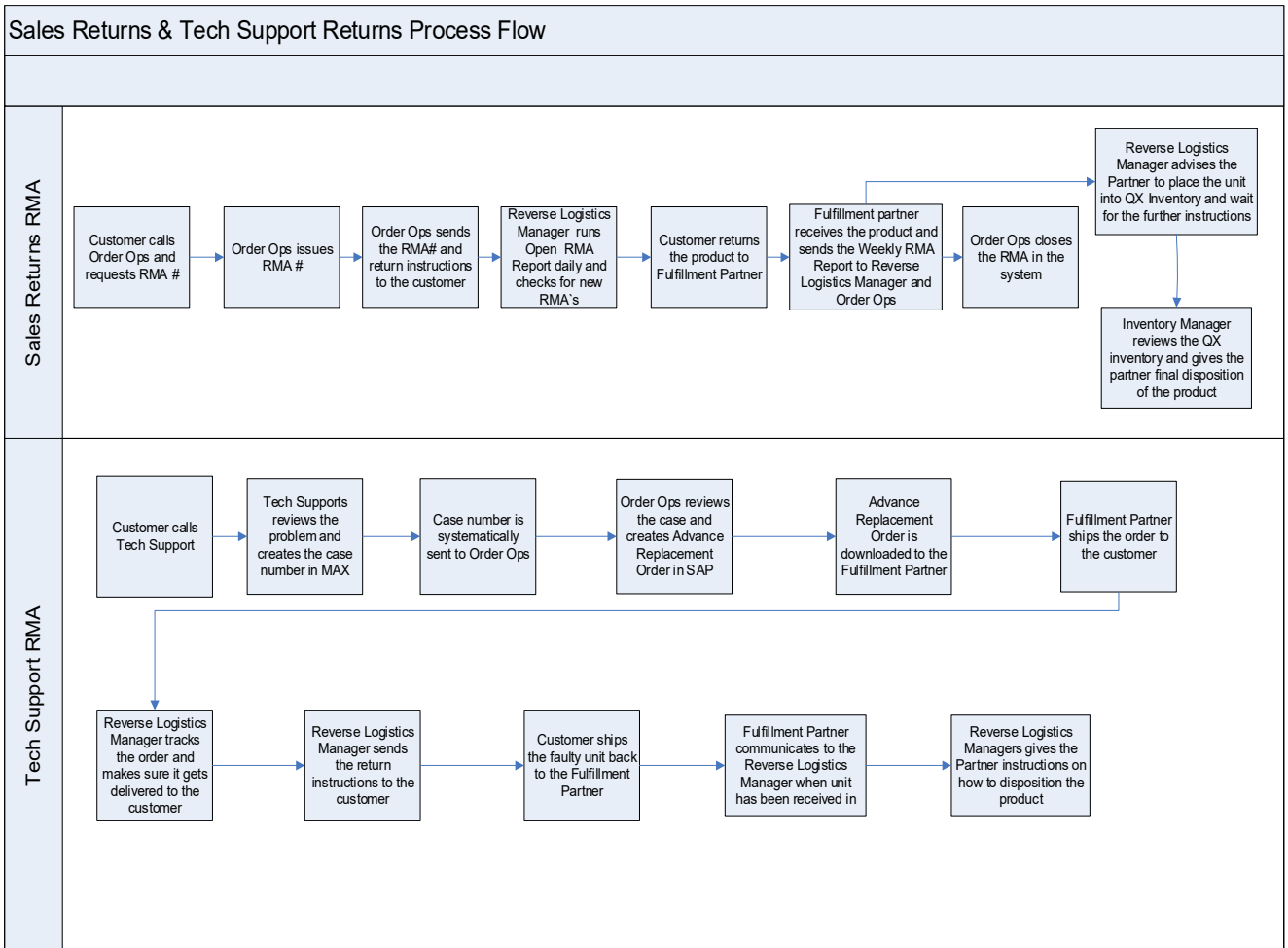


Appendix 3

Scrap process - Wisetek (EMEA)



Appendix 4



Appendix 5

Support Documentation References

- [McAfee Hardware Support Handbook](#)
 - [McAfee Support Hardware Locations](#)
 - [McAfee Certificate of Destruction](#)
 - [McAfee Materials Retention Statement](#)

Copyright © 2017 McAfee, LLC

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

