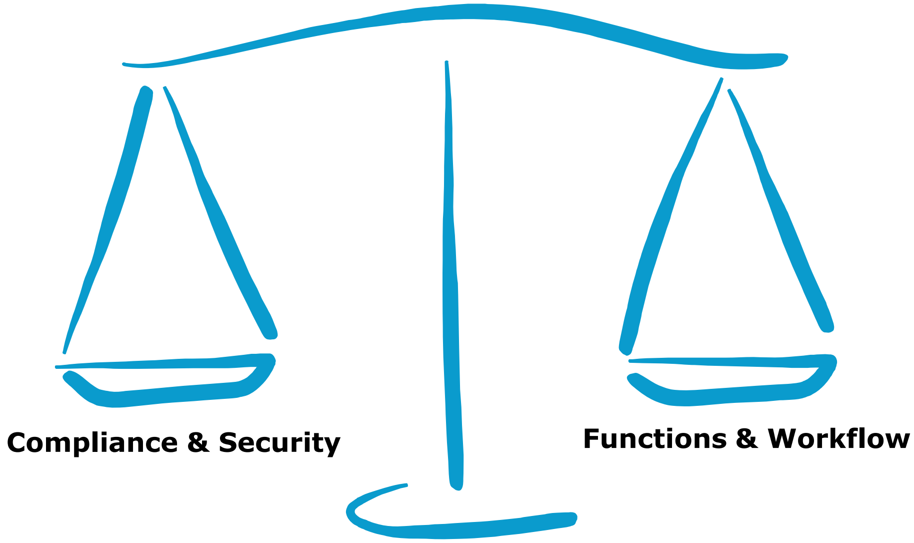
Applied Security and Compliance

There is a balance required when providing proper Compliance and Security features without impeding on functionality and workflows.

Kyocera can help you find the right balance.

Kyocera offer a complete line of multifunction and single function print devices that have the ability to meet your workflow, compliance and security requirements.



KYOCERA

Applied Security and Compliance

+ The following security processes enable Kyocera devices to be secure inside the clients network and ensure the MFP cannot be used as a platform to launch malicious software or to use the MFP as a conduit to encroach into a client’s network.

To sum it up, the Kyocera device is a stable, safe and secure device and platform on their network.

Secure Boot

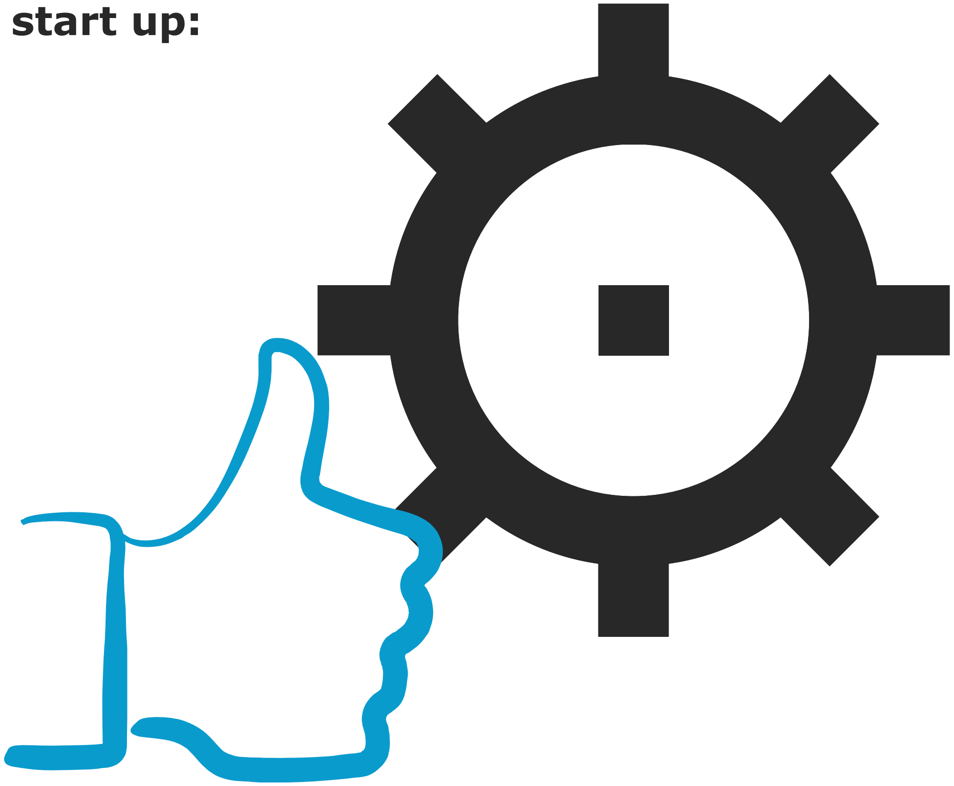
Secure Boot performs a comprehensive check to ensure the following areas are at 100% integrity at start up:

+ Firmware & Bios

+ Kyocera Proprietary LINUX Platform

+ Kyocera Proprietary Java Platforms

When utilizing **Kyocera Fleet Services**, if a secure boot error occurs central monitoring will **immediately notify** and the firmware will be **updated remotely** in a quick and effective manner.



KYOCERA

Kyocera Run Time Integrity

+ **Run Time Integrity** checks are performed periodically to Safeguard the Firmware, including the Java, LINUX Platforms and Bios has not been compromised during the operation of the MFP.

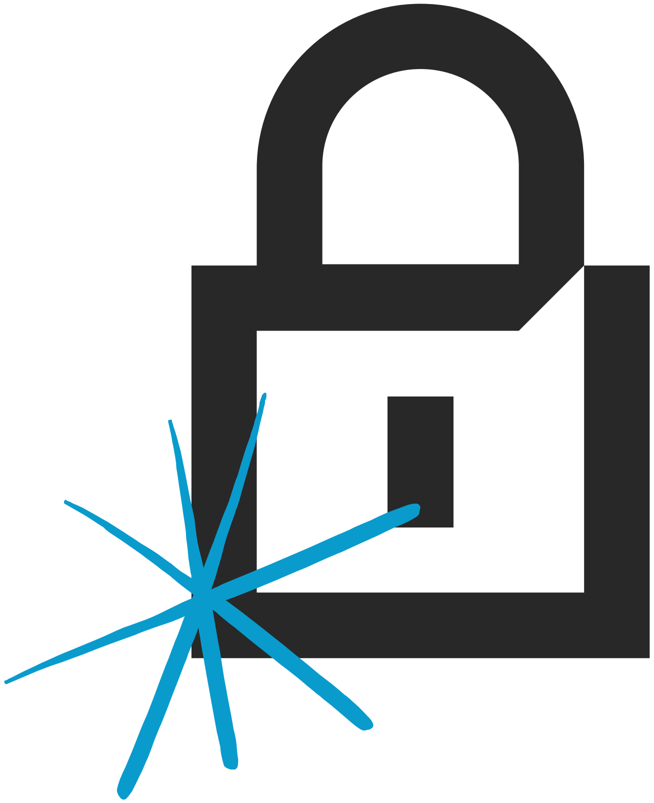
When utilizing **Kyocera Fleet Services**, if a Run Time Integrity error occurs, central monitoring will **immediately notify** and the firmware will be **updated remotely** in a quick and effective manner.

Trusted Platform Module

Kyocera TPM is a security chip set that applies a Cipher Key on the Kyocera Data Security Kit for additional layer of protection for the following:

- + HyPAS applications
- + Address book
- + Logs
- + Image data
- + Document box and user lists.

Kyocera's TPM technology is **chip set**, **cannot be compromised** and provides a second layer of security that is applied to all information on HDD. If the HDD is removed from the Kyocera Device, the information can not be accessed due to the requirement of the Physical TPM Chip to read the data.



KYOCERA

Kyocera End of Life

+ Kyocera offers a unique security feature on select MFP’s. The **End of Life Data Sanitization (EOLDS)** is designed to ensure your Kyocera MFP will be completely cleaned of all user level data before the device is disposed or removed from your locations, saving valuable time and resources.

+ **EOLDS** can offset the need to schedule a technical person from the dealership to directly interface with the MFP to ensure the machine has all your information removed at the end of the MFPs life, while also eliminating the need to remove the hard drive to perform a low level format that will require a re-install after the process. **How can we assure this?**

Kyocera End of Life

End of Life Protocols

Secure option for your customers concerning end of life data sanitization.

Industry leading 6-step Kyocera MFP Sanitization:

1. Set sanitization by calendar date for end of lease or life
2. Auto-generate an e-mail to administers indicating the sanitization process has started.
3. DoD 5220.22-M Three times overwrite with low level format.
4. Creates a printed completion confirmation at the completion of the sanitization process.
5. Permanently indicates in display that Sanitization mode was performed
6. Disables the MFP from further use

Reactivation of formatted MFP for Lease returns – only possible by authorized Kyocera Technician

Kyocera End of Life

End of Life Architecture

Completely erases all user data on all systems within the MFP and returns to factor defaults.

- + Hard Drive & RAM
- + Address Books
- + Certificates & Authentication
- + Network communication and configuration information
- + All Fax, Scan, Copy, Print Information
- + Machine & Display settings
- + Machine information Base Customer Data (MIB)

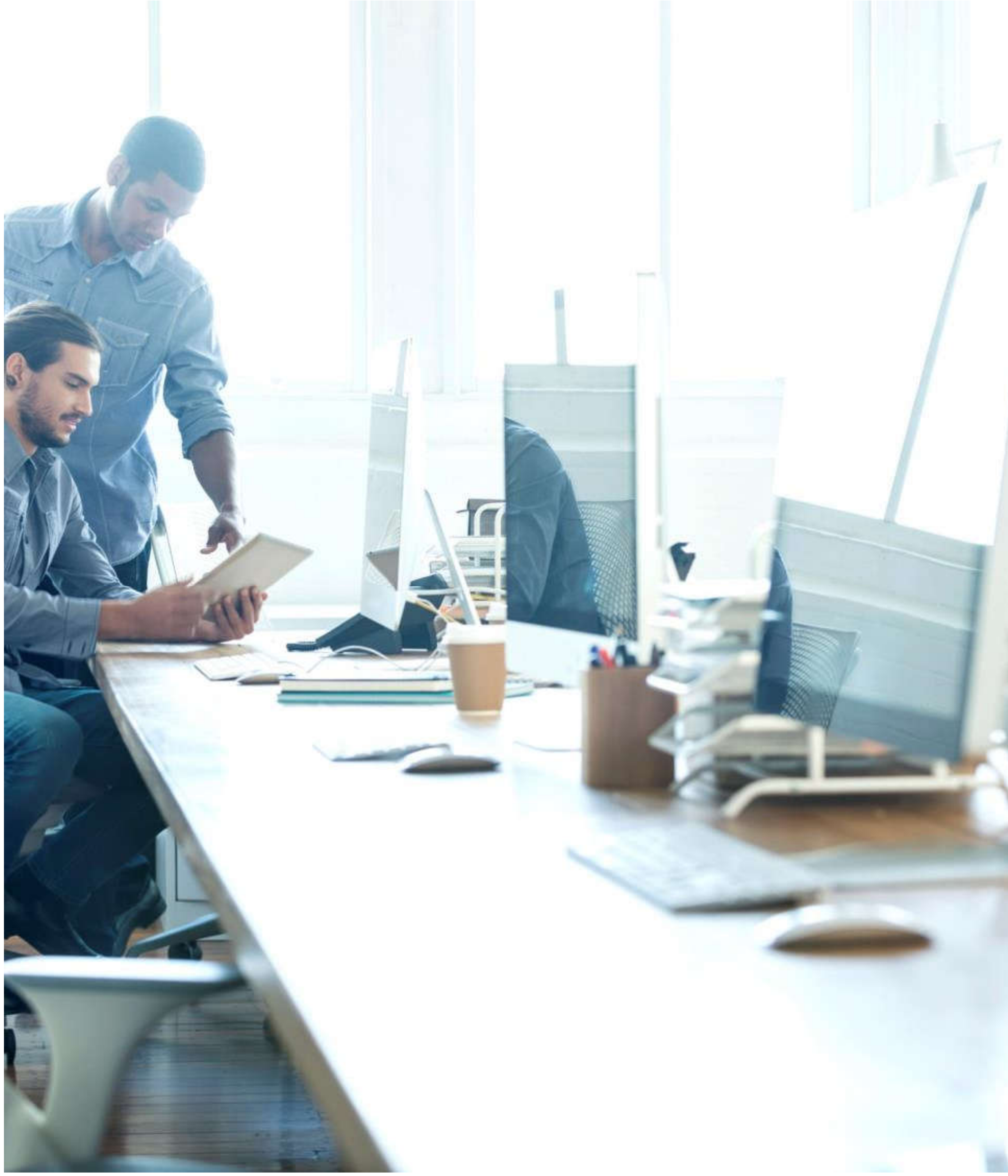
Compliances:

- + U.S. DoD 5220.22-M Sanitization Methods
- + Common Criteria EAL Level 3 same as Kyocera MFP
- + MFP and Process IEEE 2600 certified
- + Meets US Security Technical Implementation Guide (STIG) Level Authentication for Management

Kyocera End of Life

Management for End of Life Sanitization

- **Only the administrator with the highest level access to MFP will be able to configure the EOLDS function.**
- Access to the EOLDS can be set and managed remotely utilizing the MFP’s Administrative **Command Center.**
- Access to Kyocera Command Center requires a user name and password which can be configured up to 64 charters for each, which **exceeds the US Government STIG Standards** for login to authenticate (US STIG Requirement of 15 Characters with Caps, Numeric and Special Characters).
- When the End of Life Sanitization starts, up to three **(3) administrators can be e-mailed** the process is being executed.



Kyocera End of Life
Administrative E-Mail Notification

Mail subject:

TASKalfa 3252ci event mail
[Sanitization]

Mail body:

```
Equipment ID:
Model Name:             TASKalfa 3252ci
Serial Number:          W2R6400022
MeterDate:             Tue 13 Feb 2018
08:52:38
Counters by Function:
 Printed Pages:
  Copier:              811
  Printer:            11248
  FAX:                0
  Total:             12059
 Scanned Pages:

  Total:             12059
-------------------
TASKalfa 3252ci
[00:17:c8:27:af:2e]
-------------------
```

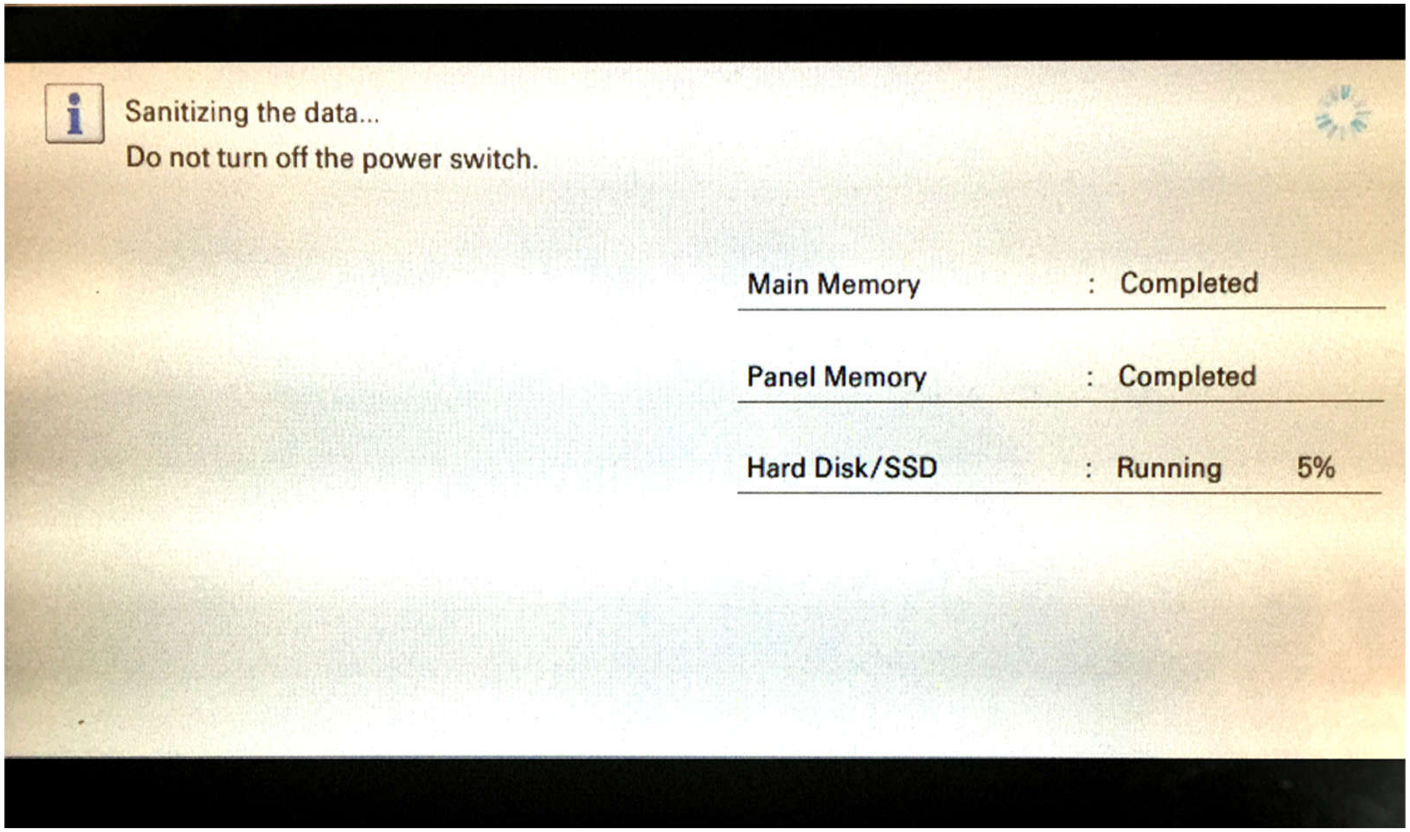
When process starts it will disable the MFP and take estimated 4 hours.

Note: Once process is underway, it is not possible to stop or cancel EOLDS.

Kyocera End of Life

Processing Display Notification

Display while overwriting and formatting all data.



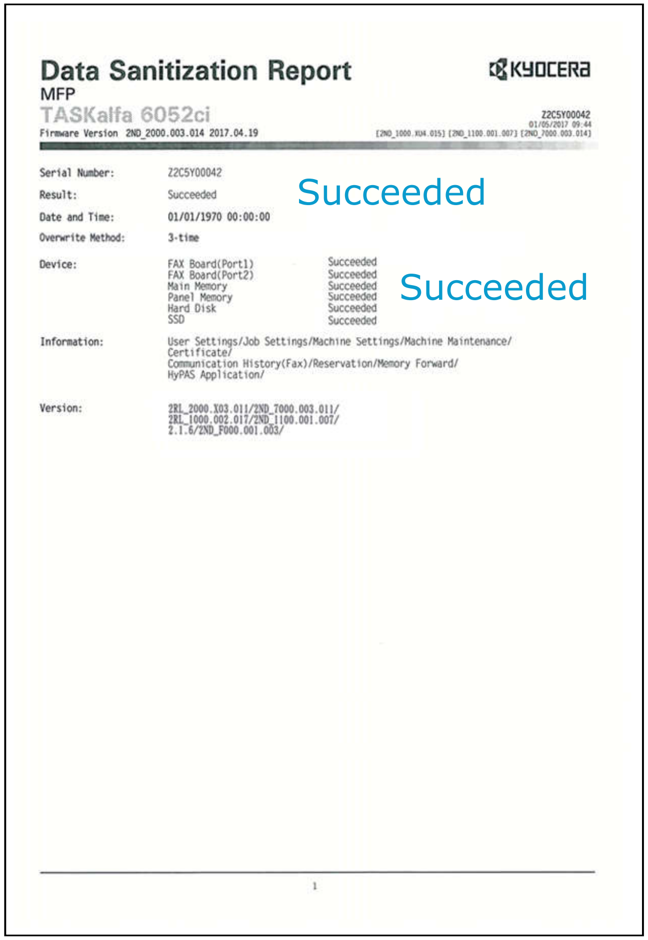
Sanitizing the data...

Do not turn off the power switch.

Main Memory	:	Completed	
Panel Memory	:	Completed	
Hard Disk/SSD	:	Running	5%

Confirmation Print-Out Report

Successful

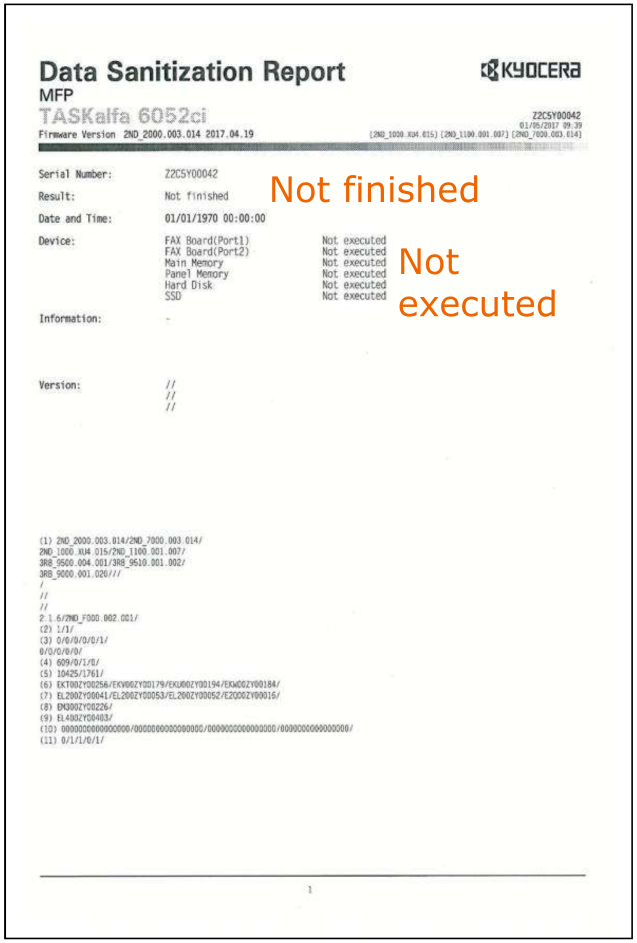


```
Data Sanitization Report                                        KYOCERA
MFP
TASKalfa 6052ci                                                 Z2C5Y00042
                                                          01/05/2017 09:44
Firmware Version  2ND_2000.003.014 2017.04.19   [2ND_1000.XU4.015] [2ND_1100.001.007] [2ND_7000.003.014]

Serial Number:      Z2C5Y00042
Result:             Succeeded
Date and Time:      01/01/1970 00:00:00
Overwrite Method:   3-time

Device:             FAX Board(Port1)         Succeeded
                    FAX Board(Port2)         Succeeded
                    Main Memory              Succeeded
                    Panel Memory             Succeeded
                    Hard Disk                Succeeded
                    SSD                      Succeeded

Information:        User Settings/Job Settings/Machine Settings/Machine Maintenance/
                    Certificate/
                    Communication History(Fax)/Reservation/Memory Forward/
                    HyPAS Application/

Version:            2RL_2000.X03.011/2ND_7000.003.011/
                    2RL_1000.002.017/2ND_1100.001.007/
                    2.1.6/2ND_F000.001.003/

                                     1
```

Succeeded

Succeeded

Failure



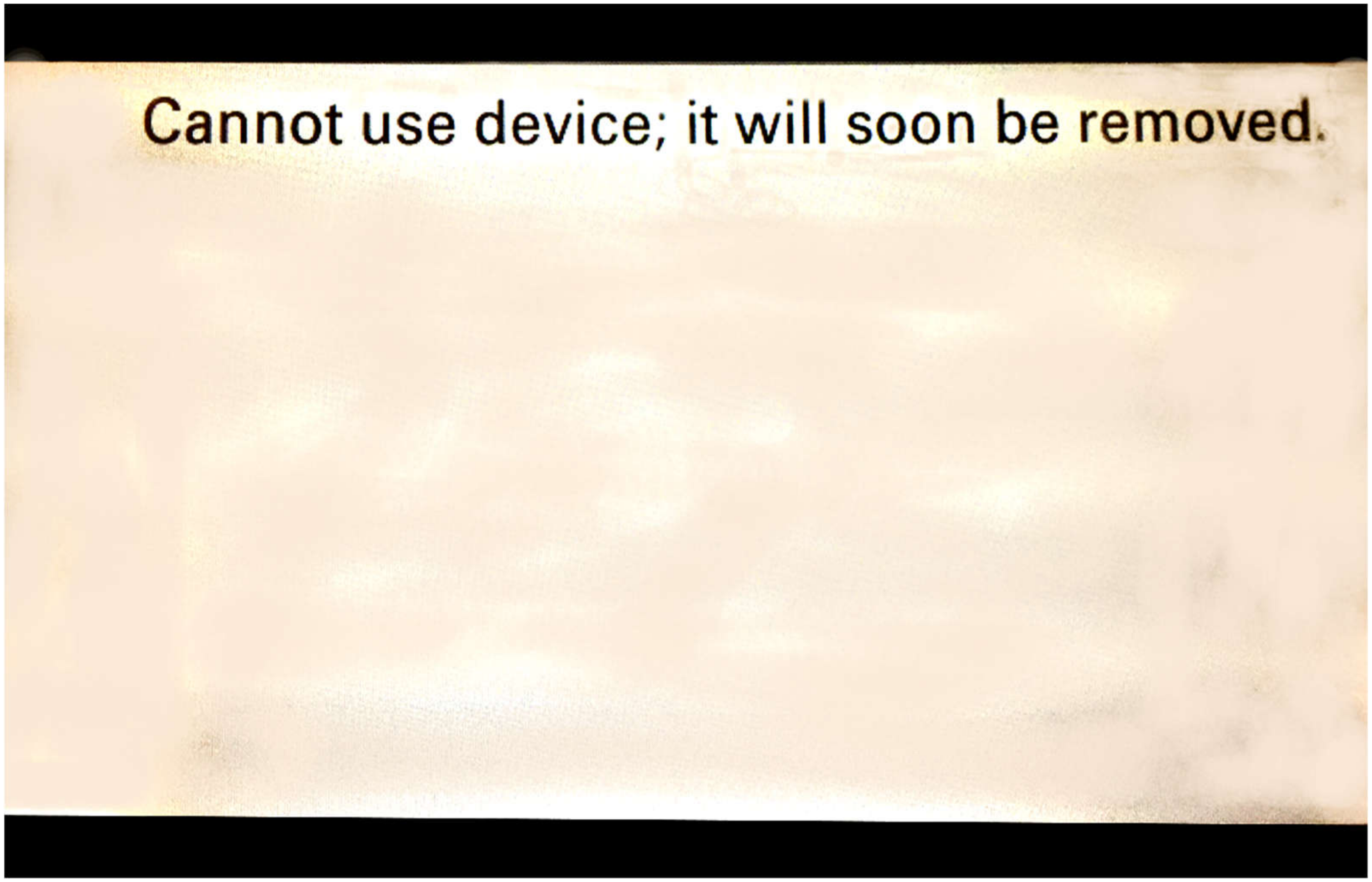
```
Data Sanitization Report                                        KYOCERA
MFP
TASKalfa 6052ci                                                 Z2C5Y00042
                                                          01/05/2017 09:39
Firmware Version  2ND_2000.003.014 2017.04.19   [2ND_1000.XU4.015] [2ND_1100.001.007] [2ND_7000.003.014]

Serial Number:      Z2C5Y00042
Result:             Not finished
Date and Time:      01/01/1970 00:00:00
Device:             FAX Board(Port1)         Not executed
                    FAX Board(Port2)         Not executed
                    Main Memory              Not executed
                    Panel Memory             Not executed
                    Hard Disk                Not executed
                    SSD                      Not executed
Information:        -


Version:            //
                    //
                    //


(1) 2ND_2000.003.014/2ND_7000.003.014/
2ND_1000.XU4.015/2ND_1100.001.007/
3R8_9500.004.001/3R8_9510.001.002/
3R8_9000.001.020///
/
//
//
2.1.6/2ND_F000.002.001/
(2) 1/1/
(3) 0/0/0/0/0/1/
0/0/0/0/0/
(4) 609/0/1/0/
(5) 10425/1761/
(6) EKT00ZY00256/EKV00ZY00179/EKU00ZY00194/EKW00ZY00184/
(7) EL200ZY00041/EL200ZY00053/EL200ZY00052/E2000ZY00016/
(8) EM300ZY00226/
(9) EL400ZY00403/
(10) 0000000000000000/0000000000000000/0000000000000000/0000000000000000/
(11) 0/1/1/0/1/

                                     1
```

Not finished

Not executed

Kyocera End of Life

Display Disable Notification



Cannot use device; it will soon be removed.

Can only be reset by Kyocera Certified Technician.

KYOCERA

Device Login Error Lockout

Kyocera Devices can be set to lockout users after a set number of failed attempts and log the users NIC, MAC and IP Address. To ensure that no one able into hack into Kyocera device to change setting.

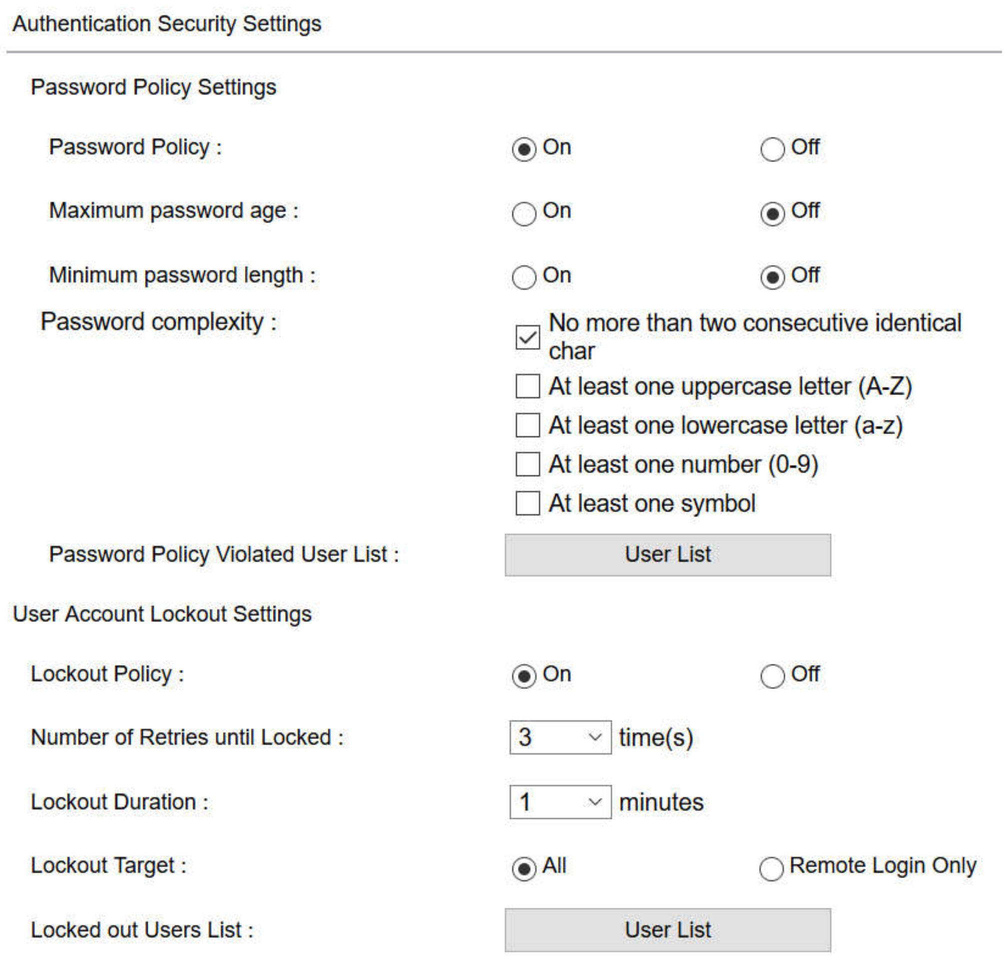
Kyocera devices also create detailed log file for users and administrators.

System Log reports by:

- User login
- IP address
- PC/Device name

Type of reports:

- Audit Job Log
- User Login Log
- Security Com Error Log
- Fax Logs/Email Job Log
- Log Management Tool



Authentication Security Settings

Password Policy Settings

Password Policy :	● On	○ Off
Maximum password age :	○ On	● Off
Minimum password length :	○ On	● Off
Password complexity :	☑ No more than two consecutive identical char ☐ At least one uppercase letter (A-Z) ☐ At least one lowercase letter (a-z) ☐ At least one number (0-9) ☐ At least one symbol	
Password Policy Violated User List :	User List	

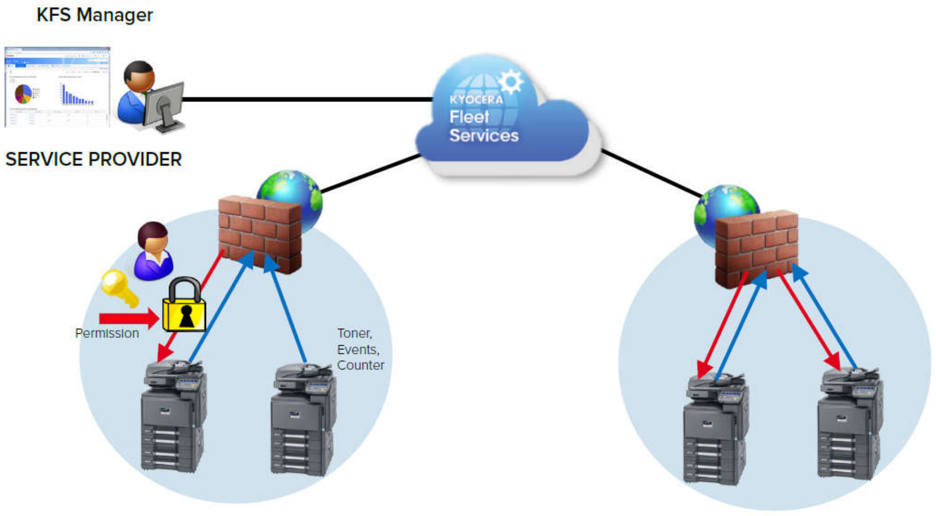
User Account Lockout Settings

Lockout Policy :	● On	○ Off
Number of Retries until Locked :	3 time(s)	
Lockout Duration :	1 minutes	
Lockout Target :	● All	○ Remote Login Only
Locked out Users List :	User List	

Kyocera Fleet Management Advantage

Key Points

- **Centralized Management** of fleet in real time
- Remote **diagnostics** and device resets
- Remote firmware **updates**
- Remote **display view** and navigation
- **Recognized information security** controls and industry-specific compliance
  - ISO 270001
  - HIPAA
  - FedRAMP
  - SOC 1 and SOC 2
  - Australia CCSL (IRAP)
  - UK G-Cloud
  - Singapore MTCS



CUSTOMER A

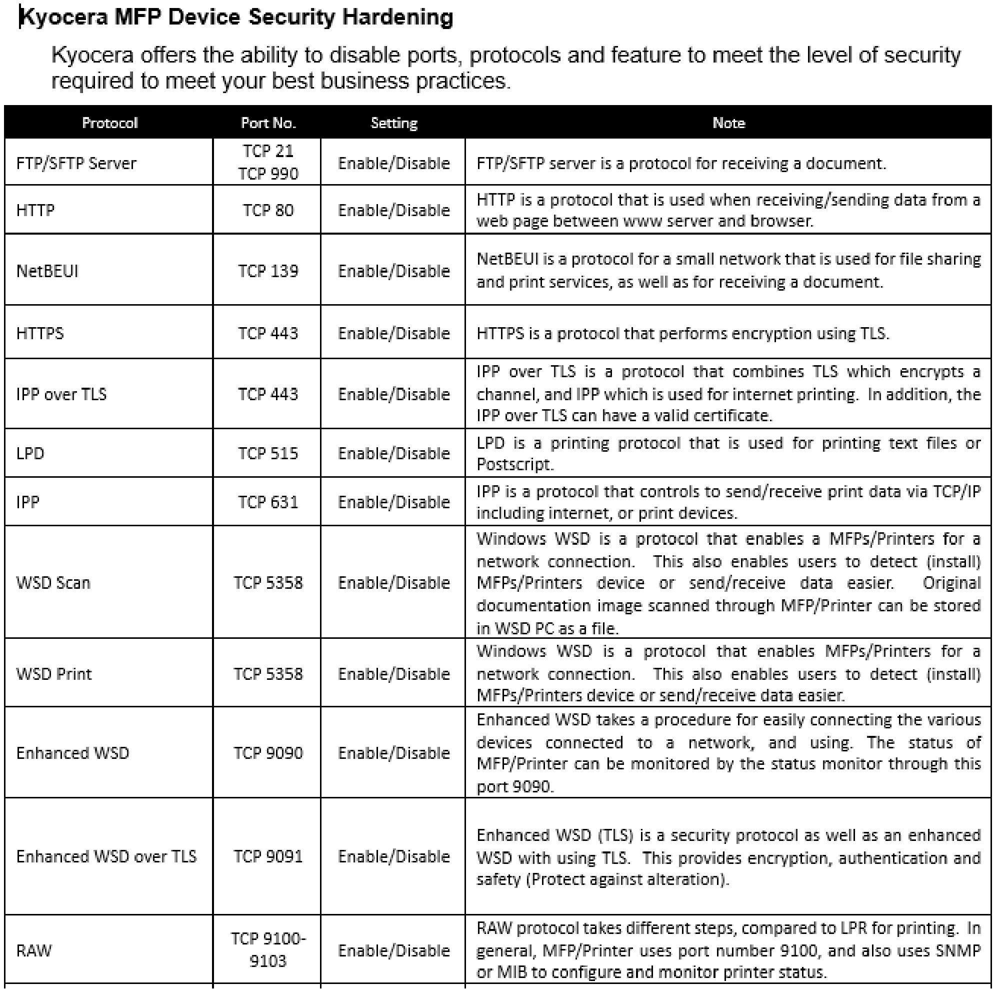
Remote Maintenance can be performed only when the customer A is permitted that using CCRX but Data Collection (Counter, toner level, device log) is always

CUSTOMER B

Remote Maintenance is always ON and can be performed on the devices in customer B as well as the Data Collection (Counter, toner level, device log)

Security Hardening of Device

Kyocera provides a list of all ports and protocols that can be enabled or disabled. Working with the client we can determine the optimal configuration of the devices and are able to set the standard across the fleet remotely utilizing the KFS tools. Over 40 different configuration and security selection can be set on the Kyocera Device.



Kyocera MFP Device Security Hardening

Kyocera offers the ability to disable ports, protocols and feature to meet the level of security required to meet your best business practices.

Protocol	Port No.	Setting	Note
FTP/SFTP Server	TCP 21 TCP 990	Enable/Disable	FTP/SFTP server is a protocol for receiving a document.
HTTP	TCP 80	Enable/Disable	HTTP is a protocol that is used when receiving/sending data from a web page between www server and browser.
NetBEUI	TCP 139	Enable/Disable	NetBEUI is a protocol for a small network that is used for file sharing and print services, as well as for receiving a document.
HTTPS	TCP 443	Enable/Disable	HTTPS is a protocol that performs encryption using TLS.
IPP over TLS	TCP 443	Enable/Disable	IPP over TLS is a protocol that combines TLS which encrypts a channel, and IPP which is used for internet printing. In addition, the IPP over TLS can have a valid certificate.
LPD	TCP 515	Enable/Disable	LPD is a printing protocol that is used for printing text files or Postscript.
IPP	TCP 631	Enable/Disable	IPP is a protocol that controls to send/receive print data via TCP/IP including internet, or print devices.
WSD Scan	TCP 5358	Enable/Disable	Windows WSD is a protocol that enables a MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier. Original documentation image scanned through MFP/Printer can be stored in WSD PC as a file.
WSD Print	TCP 5358	Enable/Disable	Windows WSD is a protocol that enables MFPs/Printers for a network connection. This also enables users to detect (install) MFPs/Printers device or send/receive data easier.
Enhanced WSD	TCP 9090	Enable/Disable	Enhanced WSD takes a procedure for easily connecting the various devices connected to a network, and using. The status of MFP/Printer can be monitored by the status monitor through this port 9090.
Enhanced WSD over TLS	TCP 9091	Enable/Disable	Enhanced WSD (TLS) is a security protocol as well as an enhanced WSD with using TLS. This provides encryption, authentication and safety (Protect against alteration).
RAW	TCP 9100-9103	Enable/Disable	RAW protocol takes different steps, compared to LPR for printing. In general, MFP/Printer uses port number 9100, and also uses SNMP or MIB to configure and monitor printer status.