GSD. Global – Mobile Phone – Lost or Stolen Mobile Devices

Article ID: KB0039794
Created: 2024-12-19 14:03:36
Updated: 2024-12-19 14:03:36
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/acaf843397d74958f7e3bb8fe153afe3', 'value': 'acaf843397d74958f7e3bb8fe153afe3'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/50a39c48c3ca1a100acd33001501314c', 'value': '50a39c48c3ca1a100acd33001501314c'}

General Information:

Possible symptoms/errors:

User’s device has been lost/stolen and want to know necessary steps that should be taken in this situation.

Alternative names of the system:

LostStolenDevice

IMPORTANT NOTICE:

N/A

Solution:

Mobile devices allows users to conveniently access documents and do some work-related tasks on the go. However, losing a device can be a hassle to every user.

Fresenius Medical Care Global DTI ServiceDesk

Advise user to notify their manager and their local Administrator.Inform user to send an email to GlobalDTIServiceDesk@freseniusmedicalcare.com or call Global Service desk

User must report that their Fresenius owned device is lost or stolen and provide the following information

Email addressPhone Number (if applicable)Device Type

Their device will be set to a quarantine mode that all Fresenius data is not accessible

Advise them to Cancel / Stop Cellular Service (if applicable) by contacting their mobile provider

Or

MobileIron Self-Service Portal - available 24/7

Advise user to notify your manager and their local Administrator.Inform user to login using one of the following links and wipe the device:

Primary Link: https://emmcore.hg.fresenius.de/mifs/user/login.jsp (VPN needed)Secondary Link: https://emm.fresenius.com/mifs/user/login.jsp (VPN needed)

When Primary link does not work, then advise to try with the Secondary link.To login, user must use:

user’s Fresenius email addressuser’s Windows password

Advise them to Cancel / Stop Cellular Service (if applicable) by contacting their mobile provider

Cyber Security Procedure:

In any case of a lost Laptop, Hard drive, USB Stick, SD Card, Mobile Device or any data medium the agent needs to perform the steps described below and also initiate process Cyber Security Procedure .

Is the Incident data protection relevant ?

If yes: continue with Procedureif no: stop procedure here

Notifying Data Protection Team about the Incident:

In case an incident is suspicious to be data protection relevant the Fresenius Data Protection team needs to be notified by creating a ServiceNow Ticket (also in case initial Incident was in Solution Manager), following the steps below:

Go to ServiceNowOpen the relevant IncidentCreate a follow up Incident Ticket (Burger Menu Top left; create follow-up Incident)Apply the global Template “Data Protection”Add a work note why the Incident is suspicious to be data protection relevantSubmit the Ticket

Acceptance criteria: · Work note description with reason why Incident is suspicious added · Ticket assigned to Assignment Group "Int_WW_Data Protection_SLS_FSE"

Assignment Group:

Ext_WW_Mobile-Workplace_SLS_CapgeminiInt_WW_Data Protection_SLS_FSE

Ticket Creation:

Template: N/ACategorization:

Configuration Item: N/ACategory: N/ASubcategory: N/A

Important Links:

N/A