

Policy on Stolen Machines

Actions to be taken when Enrolment Station machine (laptop/desktop) gets stolen:

1. EA will register an FIR for the stolen machine.
2. EA will immediately inform Registrar, UIDAI Regional Office, UIDAI techsupport, UIDAI Contact Centre (where resident re-enrolment is required). The details that may be required by various stakeholders are captured in Table I.
3. CIDR will then deregister the stolen machine and block any enrolment packets from being processed that have a date and time stamp after the machine was stolen.

Information Item	Registrar	Regional Office	UIDAI Techsupport	UIDAI Contact Centre
Date and Approximate Time when machine was stolen	✓	✓	✓	✓
Registrar Name and Code		✓	✓	✓
EA name and Code	✓	✓	✓	✓
Address of the Centre from where machines were stolen	✓	✓	✓	✓
Station ID of all stolen machines			✓	✓
Machine ID of all stolen machines(desired)			✓	
Last Operator/Supervisor who operated on machine/s before they was/were stolen			✓	
EID of the last resident enrolled on the machine/s			✓	
Location codes filled in the machine/s (optional)			✓	
List of all EIDs whose data have been lost and need to re-enroll (alternatively provide Centre address ,Station number and specify the time period				✓

4. Handling resident data lost in stolen machines:

- a. To minimize the impact of lost data due to stolen machines, it is critical that **EAs upload packets to CIDR on timely basis and take regular backup of machines.**
- b. The data packets must be transferred to CIDR at the end of day or two days. In difficult to reach areas or due to other constraints, this time may be 4-5 days. Timely upload is an measure that can help loss of data packets.
- c. UID has prescribed twice a day backup of all stations. If such regular back up is taken by EA for all active stations, it will help in providing immediate backup for lost data of stolen machines.

If EA already has backup of all packets, he can utilize the same for loading in CIDR.

<Tech team to define broad guidelines for EA to follow when utilizing backup data for uploading data packets in CIDR>.

[Handwritten Signature]
20/7

5. **If back up has not been taken by EA, a much more tedious process needs to be followed by EA to re-enroll the residents which is as follows:**
 - a. Pull out the Resident Consents for the stolen station. Note that UIDAI DMS process prescribes station wise file to be maintained by EA for all resident documents.
 - b. Take into consideration those residents' consent that are after the last export date/ last backup taken by EA, whichever is latest. As a best practice EA should maintain a Register for all exports and backup taken for each machine which can be referred to in case of any eventuality.
 - c. Consult RO and Registrar. Arrange to call these residents for re-enrolment with the Registrar's and RO's consent.
 - d. There may be data packets that have been uploaded but were not received or were corrupt. If EA does not have the backup of such packets, then EA will have to arrange to call these residents as well. EAs will also have to check with tech support on such data packets.
 - e. When calling the resident for re-enrolment, communicate to the resident the need for re-enrolment and also address their anxieties related to stolen data, if any. Inform them that the data is encrypted and cannot be accessed/mis-utilized in any manner even when the machine is stolen.
 - f. Enroll the resident as per the enrolment process
 - g. When resident is re-enrolled, ask the resident to discard the previous acknowledgement. Provide latest acknowledgement to the resident and file the latest consent along with the resident documents.
 - h. In case of Introducer based enrolments, EA will also have to inform the Introducer about the re-enrolment schedule. Introducers will be required to approve the enrolment of the residents.
 - i. EA will also inform UIDAI Contact Centre about the lost/stolen machine. Provide List of all EIDs whose data have been lost and need to re-enroll, so that in case the resident calls the center he/she will get the message. Alternatively, EA can ask Contact Centre to guide residents who enrolled at the particular centre and station during specific timeframe, to re-enroll.
6. **Tech dependencies:**
 - a. Deregistration of stolen machines based on EA reporting
 - a. Block any enrolment packets from being processed that have a date and time stamp after the machine was stolen.
 - b. Develop a procedure, where upload without manifest is possible like from external back up data
 - c. Expediting processing of data packets last sent from machines before they were stolen
 - d. Techsupport will have to inform EAs on data packets that were uploaded but may need to be resent due to various reasons like packet corruption etc. at an immediate basis so that the residents can be called for re-enrolment.
 - e. CIDR to provide a report of all packets received from stolen machine so that EA can confirm any missing ids.


20/7