

## SECURITY POLICY

Written by Administrator

Tuesday, 16 September 2008 20:10 -

---

SanIndus can not access the data by maintaining the gateway or by collecting system health, our maintenance user don't take the user rights for that, just and only the facility environment. You must file by two solicitors or escrow services a backup emergency password; we can assist you in this. The data is yours, we're not interested in your data, we're interested in the continuous function of your data storage functionality. We don't have the storage encryption password. The log file of all activities therefore is accessible by a web interface. The system monitoring and maintenance is connected by a separate redundant internal set of switches which also take care of health messages. They are connected to two dedicated ADSL connections (which will be made redundant by use of wireless UMTS/CDMA connections). The external connections can be turned of if wanted (but than the firewalls within the organization of course must relay the system health messages to the monitoring engine of SanIndus and the roll-out of upgrades and patches of all system components).