Dencrypt support (24/7): +45 7211 7911

Security instructions for Dencrypt Connex

These security instructions shall be read and understood before taking the Dencrypt Connex application into use.

General security measures

Some precautions must be observed to use the application in a secure way and to avoid disclosure of confidential information. Please observe the following before taking the application into use.

Organisational security policies Before taking the app into use, the security policies and instructions for secure usage shall have been received and understood. Be aware of the classifications, which are allowed to be exchanged using the app.

Server system security The system administrator is responsible for the daily and secure operation of the Dencrypt Server System. In case of critical security incidents or unresolved vulnerabilities, the system administrator may prevent communication between specific users or may take the entire system out of operation until the issues have been resolved. In such cases, it may not be possible to establish secure communication at all or with specific users.

Secure delivery Dencrypt Connex shall only be received from the Apple Appstores. Either as a direct installation from the public Apple Appstore or from the Apple Volume Purchase Program via a Mobile Device Management system.

Device security The system security depends on a correct and secure operation of the device and the operating system and that there are no critical side-effects. Therefore, the Dencrypt Connex application and the operating system shall always be kept updated to the latest versions. In case of critical security incidents or unresolved vulnerabilities, the system administrator may prevent calls to certain user or make the entire system unavailable until the issue have been resolved.

Benign applications The Dencrypt Connex application protects information during the data transmission and when stored on the device. It does not protect against malware intercepting audio, video or text before encryption. Therefore, only benign apps shall be installed on the device. Be aware of applications, which make use of the microphone, perform screenshots, listen to the earpiece or speaker or capture keyboard strokes. Contact your system administrator for advice.

Single user device The phonebook is personal and dedicated to a specific end-user. Therefore, the device is personal and shall not be shared.

Prevent unauthorized access Protect your device against unauthorized access by always enable a passcode or biometric login.

Lost or stolen devices In case of lost or stolen devices contact your system administrator or Dencrypt support immediately.

Avoid data leakage

Observe the pre-cautions listed below to avoid information leakage, while using the application.

Avoid acoustic coupling

It is not recommended to use encrypted voice or video calls in hotel rooms and like, which cannot be considered secure. Never exchange classified information through the Dencrypt Connex application when other unclassified telephones, radio transmitters or similar are being used in the immediate proximity.

Locations which are well suited to making calls may be public spaces, where the caller's presence has not been pre-arranged. Using secure messaging is an alternative communication in areas, where acoustic coupling is possible.

Avoid screen exposure

Consider the surroundings when using Dencrypt Connex for secure video calls and messaging to ensure that the screen can not be observed by others. Be aware of the location of windows and cameras.

Other recommendations

- **Avoid using wireless headsets** - The data connection from the device to the headset is not encrypted. Use wired headsets as an alternative.
- **Avoid using handsfree car systems** - The data connection from the device to the handsfree car system is not encrypted. Disable bluetooth to avoid automatic connection and use wired headsets as an alternative.
- **Avoid using loudspeker** - Use the Dencrypt Connex loudspeaker only with care and in locations, which are protected from acoustic coupling.
- **Don't take screenshots** – Screenshots are saved unencrypted on the devices and are not deleted when the app is closed. The Dencrypt Connex will show a warning when taling screenshots.
- **Don't use copy/paste** – Don't use the copy/paste functionality during messaging.
- **Don't use voice recordings** – Voice recordings are saved unencrypted on the devices and are not deleted when the app is closed.
- **Avoid auto-correction and predictive text features** - Avoid using keyboards, which includes autocorrection or predictive text features. It is recommended to disable spell checking and predictive text from the settings menu.
- **Avoid using apps with speech recognisation** - Avoid using applications, which makes use of speech recognition features, such as speech-to-text applications.