

Biometric Data Safety Guidelines

Do's & Don'ts for Safe, Secure and Reliable Biometric Data Capture

For accurate biometric authentication and secure operation, always use the biometric scanner only for its intended purpose. Any attempt to tamper with the device, use an artificial biometric sample, bypass security controls, or perform suspicious capture attempts may result in capture rejection and further action.

☒ DO's – Always Follow These Practices

- **Visual temper validation of device.** Check device temper sticker condition and device serial number details available on bottom of device and within the RD service application to consider device not tempered and valid device to receive support
- **Keep the biometric sensor clean.** Regularly remove dust, oil, moisture and other contamination from the sensor using the cleaning method recommended for your device.
- **Always use a clean finger for biometric data capture.** Ensure the finger is free from excessive dirt, oil, grease, ink, dust or other substances before scanning.
- **Always use the device for live biometric data capture.** The biometric scanner should only be used to capture a genuine, live biometric data directly from the actual user.
- **Place the finger properly on the sensor.** Position the centre of the finger over the scanning area and provide sufficient contact without excessive pressure.
- **Keep the finger dry if it is wet or sweaty.** Wipe the finger before scanning to help improve biometric data capture quality.
- **Use another enrolled finger if the selected finger is injured or difficult to capture.** Cuts, damaged skin or worn ridge patterns can affect capture quality.
- **Always operate the device under proper supervision.** In operator-assisted environments, biometric data capture should be carried out under the supervision of an authorised operator.
- **Allow only authorised and trained personnel to operate the device.** Operators should understand the approved biometric capture procedure and basic troubleshooting process.

- **Inspect the device before use.** Check the sensor, enclosure, cable, connector and other visible parts for damage, unusual marks or signs of tampering.
- **Stop using the device if tampering is suspected.** Immediately report any broken enclosure, altered seal, damaged sensor, suspicious modification or unusual behaviour.
- **Contact authorised support after repeated genuine capture failures.** If a valid biometric capture fails multiple times, stop continuously retrying and contact the authorised technical support team.
- **Always repair or service the device through an authorised service centre.** Device servicing and internal component replacement should only be performed by the manufacturer or an authorised service partner.
- **Use only approved software, drivers and firmware.** Install software and updates only from authorised or officially approved sources.
- **Use genuine or approved cables and accessories.** Incorrect power supplies, USB cables, adapters or accessories may affect device performance and reliability.
- **Follow the prescribed biometric capture workflow.** Perform biometric data capture only through the authorised application or approved software environment.
- **Report suspicious activity immediately.** Suspected fake or artificial biometric samples, unauthorised device handling, repeated abnormal capture attempts or unusual device behaviour should be reported to the authorised support or security team.
- **Protect the device from physical damage.** Keep it away from excessive heat, water, corrosive chemicals, heavy impact and unsuitable operating conditions.
- **Follow the manufacturer's recommended cleaning procedure.** Avoid any cleaning method that could damage the biometric sensor.

DON'Ts – Strictly Avoid These Actions

- **Never open or dismantle the biometric scanner yourself.** Opening the device may damage internal components, compromise device security and invalidate applicable warranty or certification.
- **Never tamper with the device.** Do not drill, cut, modify, rewire, alter, bypass or interfere with the scanner, sensor, enclosure, electronic components or communication mechanism.
- **Never use a device that appears tampered with.** A modified, damaged or suspicious device should immediately be removed from operation and reported.
- **Never give the device to an unauthorized repair or service centre.** Unauthorised repairs or component replacement can affect device security, calibration and reliability.
- **Never use an artificial, fabricated or material-based biometric sample.** Do not attempt biometric data capture using moulded, printed, replicated, synthetic or fabricated biometric representations.
- **Never attempt to spoof the biometric scanner.** Any effort to impersonate another individual or deceive the biometric capture process is strictly prohibited and discouraged.
- **Never use another person's biometric data without legitimate authorized .**
- **Never try to use stored or previously captured biometric data as a substitute for a genuine live biometric data capture.**
- **Never continuously perform multiple failed biometric data capture attempts.** If genuine biometric data capture repeatedly fails, stop and identify the cause or contact authorized support.
- **Never intentionally perform repeated failed or suspicious capture attempts to test, manipulate or bypass the biometric system.**
- **Never modify the scanner's firmware, drivers or internal configuration using unofficial or unauthorized tools.**
- **Never install or use unverified third-party biometric software with the device.**
- **Never attempt to bypass biometric authentication using malicious, third-party or unauthorized software.**

- **Never attempt to bypass an authentication rejection by altering, modifying, tampering with or manipulating the biometric scanner/application.**
- **Never share your biometric scanner with another nauthorized person, operator or nauthorized.** The device should remain under the custody and control of the nauthoriz user or nauthorized who have purchased the device.
- **Never give the biometric scanner on rent, lease or temporary use to another person, operator, agency or nauthorized unless specifically nauthoriz under the applicable deployment policy.**
- **Never hand over the device to an unknown /unauthorized person for testing, inspection, repair, configuration or troubleshooting.**
- **Never pour cleaning liquid directly onto the biometric sensor.** Use only the recommended cleaning procedure.
- **Never clean the sensor using sharp, rough or abrasive objects.** These may scratch or permanently damage the sensing surface.
- **Never press the sensor using fingernails, pens, tools or other hard objects.**
- **Never apply excessive force while scanning.** Normal finger contact is sufficient.
- **Never use the device if the cable, connector, housing or sensor is significantly damaged.**
- **Never disconnect or interrupt the device during an nauthoriz firmware or software update unless specifically instructed by technical support.**
- **Never expose the scanner to unnecessary water, excessive moisture, extreme temperatures or corrosive substances.**
- **Never leave the device unattended where nauthorized persons may access, replace, modify, misuse or tamper with it.**
- **Never ignore abnormal device behaviour.** Unexpected errors, unusual capture behaviour or repeated genuine biometric capture failures should be reported rather than continuously retried.

IMPORTANT SECURITY & ANTI-SPOOFING WARNING

ONLY GENUINE LIVE BIOMETRIC DATA SHOULD BE USED

The biometric scanner must be used only for legitimate live biometric data capture from the actual individual.

Strictly avoid:

- Artificial or fabricated biometric samples
- Replicated or copied biometric samples
- Material-based biometric impressions
- Unauthorised biometric presentations
- Device tampering or modification
- Malicious or unauthorised third-party software
- Attempts to bypass authentication
- Repeated intentional failed capture attempts
- Unauthorised opening or servicing of the device
- Sharing or renting the device to unauthorised persons
- Attempts to impersonate another person

Repeated suspicious or failed attempts may be logged, rejected, temporarily restricted or escalated according to the configured security policy.

If a genuine user experiences repeated biometric data capture failures:

STOP RETRYING → CHECK/ CHANGE FINGER → CLEAN SENSOR → RETRY CORRECTLY → CONTACT AUTHORISED SUPPORT

Do not attempt to solve authentication failure by opening, modifying, tampering with or using unauthorised software with the device.

Recommended Procedure After Repeated Biometric Capture Failure

1. **STOP** continuous biometric data capture attempts.
2. **CHECK** whether the finger is clean, dry and properly positioned.
3. **CLEAN** the sensor using the recommended cleaning method.
4. **TRY** another legitimately enrolled finger, where permitted.
5. **INSPECT** the device for visible damage or signs of tampering.
6. **REPORT** continued failure to the authorised operator or administrator.
7. **CONTACT AUTHORISED SUPPORT** if the problem continues.

Never open, modify, tamper with or use unauthorised software to overcome a biometric authentication failure.

Remember

CLEAN SENSOR • CLEAN FINGER • LIVE BIOMETRIC DATA • AUTHORISED OPERATOR • AUTHORISED SERVICE

Use the biometric scanner only for genuine biometric capture. Never spoof, tamper, modify, share, rent or misuse the device.