MANTRA
Innovation that counts

OPERATOR GUIDE

2026 EDITION

BIOMETRIC DATA

SAFETY GUIDELINES

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

OPERATOR | ENGLISH + HINDI

Secure biometric capture starts with correct device handling, authorised use and genuine live biometric data.

MANTRA SOFTECH (INDIA) PVT. LTD.

www.mantratec.com

Innovation that counts

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

EN

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.

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

- **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.

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

MANTRA
Innovation that counts

✕ 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 3nauthorized 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 3nauthorized3.**
- **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 3nauthoriz 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 3nauthorized tools.**
- **Never install or use unverified third-party biometric software with the device.**
- **Never attempt to bypass biometric authentication using malicious, third-party or 3nauthorized software.**

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

- **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 4nauthorized person, operator or 4nauthorized.** The device should remain under the custody and control of the 4nauthoriz user or 4nauthorized who have purchased the device.
- **Never give the biometric scanner on rent, lease or temporary use to another person, operator, agency or 4nauthorized unless specifically 4nauthoriz 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 4nauthoriz 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 4nauthorized 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.

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

⚠ 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.

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

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.

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

बायोमेट्रिक डेटा सुरक्षा दिशानिर्देश

सुरक्षित, संरक्षित और विश्वसनीय बायोमेट्रिक डेटा कैप्चर के लिए क्या करें और क्या न करें

सटीक बायोमेट्रिक प्रमाणीकरण और सुरक्षित संचालन के लिए बायोमेट्रिक स्कैनर का उपयोग केवल उसके निर्धारित उद्देश्य के लिए करें। डिवाइस के साथ छेड़छाड़ करना, कृत्रिम बायोमेट्रिक नमूना इस्तेमाल करना, सुरक्षा नियंत्रणों को बायपास करने का प्रयास करना या संदिग्ध तरीके से बार-बार कैप्चर करना, बायोमेट्रिक कैप्चर अस्वीकृत होने और आगे की कार्रवाई का कारण बन सकता है।

क्या करें - इन सावधानियों का हमेशा पालन करें

- **डिवाइस की छेड़छाड़-रोधी स्थिति की दृश्य जाँच करें।**

डिवाइस पर लगी टैम्पर/सुरक्षा स्टिकर की स्थिति, नीचे दिए गए सीरियल नंबर और RD Service एप्लिकेशन में उपलब्ध डिवाइस विवरण की जाँच करें। इससे यह सुनिश्चित करने में मदद मिलती है कि डिवाइस के साथ छेड़छाड़ नहीं हुई है और वह सहायता प्राप्त करने के लिए वैध है।

- **बायोमेट्रिक सेंसर को साफ रखें।**

डिवाइस के लिए अनुशंसित सफाई विधि से सेंसर पर जमा धूल, तेल, नमी और अन्य गंदगी को नियमित रूप से हटाएँ।

- **बायोमेट्रिक डेटा कैप्चर के लिए साफ उंगली का उपयोग करें।**

स्कैन करने से पहले सुनिश्चित करें कि उंगली पर अधिक धूल, तेल, ग्रीस, स्याही या अन्य पदार्थ न हों।

- **डिवाइस का उपयोग केवल वास्तविक और जीवित बायोमेट्रिक डेटा कैप्चर के लिए करें।**

बायोमेट्रिक स्कैनर से केवल वास्तविक उपयोगकर्ता का लाइव बायोमेट्रिक डेटा ही सीधे कैप्चर किया जाना चाहिए।

- **उंगली को सेंसर पर सही तरीके से रखें।**

उंगली के मध्य भाग को स्कैनिंग क्षेत्र पर रखें और बिना अधिक दबाव के पर्याप्त संपर्क बनाएँ।

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

- **गीली या पसीने वाली उंगली को पहले सुखाएँ।**

स्कैन करने से पहले उंगली पोंछ लें, इससे बायोमेट्रिक डेटा कैप्चर की गुणवत्ता बेहतर हो सकती है।

- **यदि चुनी गई उंगली घायल हो या उसका कैप्चर कठिन हो, तो दूसरी पंजीकृत उंगली का उपयोग करें।**

कट, क्षतिग्रस्त त्वचा या घिसी हुई फिंगरप्रिंट रेखाएँ कैप्चर की गुणवत्ता को प्रभावित कर सकती हैं।

- **डिवाइस का उपयोग उचित निगरानी में करें।**

जहाँ ऑपरेटर की सहायता से बायोमेट्रिक कैप्चर किया जाता है, वहाँ यह प्रक्रिया अधिकृत ऑपरेटर की निगरानी में होनी चाहिए।

- **केवल अधिकृत और प्रशिक्षित व्यक्ति को डिवाइस चलाने दें।**

ऑपरेटर को स्वीकृत बायोमेट्रिक कैप्चर प्रक्रिया और बुनियादी समस्या-निवारण की जानकारी होनी चाहिए।

- **उपयोग से पहले डिवाइस की जाँच करें।**

सेंसर, बॉडी, केबल, कनेक्टर और अन्य दिखाई देने वाले हिस्सों पर क्षति, असामान्य निशान या छेड़छाड़ के संकेत जाँचें।

- **छेड़छाड़ का संदेह हो तो डिवाइस का उपयोग तुरंत बंद करें।**

टूटी हुई बॉडी, बदली हुई सील, क्षतिग्रस्त सेंसर, संदिग्ध बदलाव या असामान्य व्यवहार की तुरंत रिपोर्ट करें।

- **वास्तविक बायोमेट्रिक कैप्चर बार-बार विफल हो तो अधिकृत सहायता से संपर्क करें।**

यदि सही तरीके से किया गया कैप्चर कई बार विफल होता है, तो लगातार प्रयास न करें और अधिकृत तकनीकी सहायता टीम से संपर्क करें।

- **डिवाइस की मरम्मत या सर्विस केवल अधिकृत सेवा केंद्र से कराएँ।**

आंतरिक पुर्जों की मरम्मत या बदलाव केवल निर्माता या अधिकृत सेवा भागीदार द्वारा किया जाना चाहिए।

- **केवल स्वीकृत सॉफ्टवेयर, ड्राइवर और फर्मवेयर का उपयोग करें।**

सॉफ्टवेयर और अपडेट केवल अधिकृत या आधिकारिक रूप से स्वीकृत स्रोतों से ही इंस्टॉल करें।

- **केवल असली या स्वीकृत केबल और एक्सेसरी का उपयोग करें।**

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

गलत पावर सप्लाई, USB केबल, एडाप्टर या अन्य एक्सेसरी डिवाइस के प्रदर्शन और विश्वसनीयता को प्रभावित कर सकते हैं।

- **निर्धारित बायोमेट्रिक कैप्चर प्रक्रिया का पालन करें।**

बायोमेट्रिक डेटा कैप्चर केवल अधिकृत एप्लिकेशन या स्वीकृत सॉफ्टवेयर वातावरण के माध्यम से करें।

- **संदिग्ध गतिविधि की तुरंत रिपोर्ट करें।**

कृत्रिम या नकली बायोमेट्रिक नमूने, अनधिकृत डिवाइस हैंडलिंग, बार-बार असामान्य कैप्चर प्रयास या डिवाइस के असामान्य व्यवहार की सूचना अधिकृत सहायता या सुरक्षा टीम को दें।

- **डिवाइस को भौतिक क्षति से सुरक्षित रखें।**

इसे अत्यधिक गर्मी, पानी, संक्षारक रसायनों, भारी झटकों और अनुपयुक्त वातावरण से बचाएँ।

- **निर्माता द्वारा सुझाई गई सफाई प्रक्रिया का पालन करें।**

ऐसी सफाई विधि का उपयोग न करें जिससे बायोमेट्रिक सेंसर को नुकसान पहुँच सकता हो।

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

क्या न करें - इन कार्यों से सख्ती से बचें

- बायोमेट्रिक स्कैनर को स्वयं कभी न खोलें या अलग-अलग हिस्सों में न करें। ऐसा करने से आंतरिक पुर्जों को नुकसान, सुरक्षा से समझौता और लागू वारंटी या प्रमाणन अमान्य हो सकता है।
- डिवाइस के साथ कभी छेड़छाड़ न करें। स्कैनर, सेंसर, बॉडी, इलेक्ट्रॉनिक पुर्जों या संचार तंत्र में ड्रिलिंग, कटिंग, बदलाव, री-वायरिंग, बायपास या किसी प्रकार का हस्तक्षेप न करें।
- ऐसा डिवाइस कभी उपयोग न करें जिसमें छेड़छाड़, बदलाव या क्षति के संकेत दिखाई दें। ऐसे डिवाइस को तुरंत उपयोग से हटाकर रिपोर्ट करें।
- डिवाइस को कभी भी अनधिकृत मरम्मत या सेवा केंद्र को न दें। अनधिकृत मरम्मत या पुर्जों का बदलाव डिवाइस की सुरक्षा, कैलिब्रेशन और विश्वसनीयता को प्रभावित कर सकता है।
- कृत्रिम, बनाए गए या किसी सामग्री से तैयार बायोमेट्रिक नमूने का कभी उपयोग न करें। मोल्ड किए गए, प्रिंट किए गए, कॉपी किए गए, सिंथेटिक या कृत्रिम बायोमेट्रिक प्रतिनिधित्व से कैप्चर का प्रयास न करें।
- बायोमेट्रिक स्कैनर को धोखा देने या स्पूफ करने का प्रयास कभी न करें। किसी अन्य व्यक्ति की पहचान का रूप धारण करना या बायोमेट्रिक कैप्चर प्रक्रिया को धोखा देना सख्त रूप से निषिद्ध है।
- उचित और वैध अनुमति के बिना किसी अन्य व्यक्ति के बायोमेट्रिक डेटा का उपयोग न करें।
- वास्तविक लाइव बायोमेट्रिक डेटा के स्थान पर संग्रहित या पहले से कैप्चर किए गए बायोमेट्रिक डेटा का उपयोग न करें।
- कई बार कैप्चर विफल होने पर लगातार प्रयास न करते रहें। वास्तविक कैप्चर बार-बार विफल हो तो कारण जाँचें या अधिकृत सहायता से संपर्क करें।
- बायोमेट्रिक प्रणाली को जाँचने, प्रभावित करने या बायपास करने के लिए जानबूझकर बार-बार विफल या संदिग्ध कैप्चर प्रयास न करें।
- अनधिकृत टूल का उपयोग करके स्कैनर के फर्मवेयर, ड्राइवर या आंतरिक कॉन्फ़िगरेशन में बदलाव न करें।
- डिवाइस के साथ अप्रमाणित तृतीय-पक्ष बायोमेट्रिक सॉफ्टवेयर इंस्टॉल या उपयोग न करें।

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

- दुर्भावनापूर्ण, तृतीय-पक्ष या अनधिकृत सॉफ्टवेयर से बायोमेट्रिक प्रमाणीकरण को बायपास करने का प्रयास न करें।
- प्रमाणीकरण अस्वीकृत होने पर स्कैनर या एप्लिकेशन को बदलकर, संशोधित करके या उसमें छेड़छाड़ करके अस्वीकृति को बायपास करने का प्रयास न करें।
- अपने बायोमेट्रिक स्कैनर को किसी अनधिकृत व्यक्ति, ऑपरेटर या संस्था के साथ साझा न करें। डिवाइस उस अधिकृत उपयोगकर्ता या संस्था की निगरानी और नियंत्रण में रहना चाहिए जिसने इसे खरीदा है।
- लागू डिप्लॉयमेंट नीति में स्पष्ट अनुमति न होने तक डिवाइस को किसी अन्य व्यक्ति, ऑपरेटर, एजेंसी या संस्था को किराए, लीज या अस्थायी उपयोग के लिए न दें।
- परीक्षण, निरीक्षण, मरम्मत, कॉन्फ़िगरेशन या समस्या-निवारण के लिए डिवाइस किसी अज्ञात या अनधिकृत व्यक्ति को न सौंपें।
- सफाई का तरल सीधे बायोमेट्रिक सेंसर पर न डालें। केवल अनुशंसित सफाई विधि का उपयोग करें।
- सेंसर को तेज, खुरदरी या घिसाव वाली वस्तुओं से साफ न करें। इससे स्कैनिंग सतह पर खरोंच या स्थायी क्षति हो सकती है।
- सेंसर को नाखून, पेन, औजार या किसी अन्य कठोर वस्तु से न दबाएँ।
- स्कैन करते समय अत्यधिक दबाव न डालें। सामान्य उंगली संपर्क पर्याप्त है।
- यदि केबल, कनेक्टर, बॉडी या सेंसर गंभीर रूप से क्षतिग्रस्त हो तो डिवाइस का उपयोग न करें।
- अधिकृत फर्मवेयर या सॉफ्टवेयर अपडेट के दौरान तकनीकी सहायता के स्पष्ट निर्देश के बिना डिवाइस को डिस्कनेक्ट या प्रक्रिया को बाधित न करें।
- स्कैनर को अनावश्यक पानी, अत्यधिक नमी, बहुत अधिक या कम तापमान तथा संक्षारक पदार्थों के संपर्क में न लाएँ।
- डिवाइस को ऐसी जगह बिना निगरानी के न छोड़ें जहाँ अनधिकृत व्यक्ति उसे बदल, संशोधित, गलत उपयोग या उसके साथ छेड़छाड़ कर सकें।
- डिवाइस के असामान्य व्यवहार को नजरअंदाज न करें। अप्रत्याशित त्रुटियाँ, असामान्य कैप्चर व्यवहार या बार-बार वास्तविक कैप्चर विफलता होने पर लगातार प्रयास करने के बजाय इसकी रिपोर्ट करें।

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

महत्वपूर्ण सुरक्षा एवं एंटी-स्पूफिंग चेतावनी

केवल वास्तविक और जीवित बायोमेट्रिक डेटा का उपयोग करें

बायोमेट्रिक स्कैनर का उपयोग केवल वास्तविक व्यक्ति के वैध और लाइव बायोमेट्रिक डेटा को कैप्चर करने के लिए किया जाना चाहिए।

इनसे सख्ती से बचें:

- कृत्रिम या बनाए गए बायोमेट्रिक नमूने
- कॉपी किए गए या दोहराए गए बायोमेट्रिक नमूने
- किसी सामग्री से बनाए गए बायोमेट्रिक निशान
- अनधिकृत बायोमेट्रिक प्रस्तुति
- डिवाइस के साथ छेड़छाड़ या बदलाव
- दुर्भावनापूर्ण या अनधिकृत तृतीय-पक्ष सॉफ्टवेयर
- प्रमाणीकरण को बायपास करने के प्रयास
- जानबूझकर बार-बार विफल कैप्चर प्रयास
- डिवाइस को अनधिकृत रूप से खोलना या सर्विस करना
- डिवाइस को अनधिकृत व्यक्तियों के साथ साझा करना या किराए पर देना
- किसी अन्य व्यक्ति की पहचान का रूप धारण करने का प्रयास
- बार-बार संदिग्ध या विफल प्रयास सुरक्षा नीति के अनुसार लॉग किए जा सकते हैं, अस्वीकृत किए जा सकते हैं, अस्थायी रूप से प्रतिबंधित किए जा सकते हैं या आगे की जाँच के लिए भेजे जा सकते हैं।

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved

यदि किसी वास्तविक उपयोगकर्ता का बायोमेट्रिक कैप्चर बार-बार विफल हो:

लगातार प्रयास रोकें → उंगली जाँचें/बदलें → सेंसर साफ करें → सही तरीके से पुनः प्रयास करें → अधिकृत सहायता से संपर्क करें

प्रमाणीकरण विफलता को दूर करने के लिए डिवाइस को खोलने, बदलने, उसमें छेड़छाड़ करने या अनधिकृत सॉफ्टवेयर का उपयोग करने का प्रयास न करें।

बार-बार बायोमेट्रिक कैप्चर विफल होने पर अनुशंसित प्रक्रिया

1. लगातार बायोमेट्रिक कैप्चर के प्रयास रोकें।
2. जाँचें कि उंगली साफ, सूखी और सही स्थिति में है।
3. अनुशंसित सफाई विधि से सेंसर साफ करें।
4. जहाँ अनुमति हो, दूसरी वैध रूप से पंजीकृत उंगली का उपयोग करें।
5. डिवाइस पर दिखाई देने वाली क्षति या छेड़छाड़ के संकेतों की जाँच करें।
6. समस्या जारी रहे तो अधिकृत ऑपरेटर या प्रशासक को सूचित करें।
7. समस्या बनी रहने पर अधिकृत सहायता टीम से संपर्क करें।

बायोमेट्रिक प्रमाणीकरण विफलता को दूर करने के लिए डिवाइस को कभी न खोलें, संशोधित न करें, उसके साथ छेड़छाड़ न करें और अनधिकृत सॉफ्टवेयर का उपयोग न करें।

याद रखें

साफ सेंसर • साफ उंगली • लाइव बायोमेट्रिक डेटा • अधिकृत ऑपरेटर • अधिकृत सेवा

बायोमेट्रिक स्कैनर का उपयोग केवल वास्तविक बायोमेट्रिक कैप्चर के लिए करें। स्पूफिंग, छेड़छाड़, अनधिकृत बदलाव, गलत उपयोग, साझा करना या किराए पर देना सख्त रूप से न करें।

© 2026 Mantra Softech (India) Pvt. Ltd. All Rights Reserved