VisionLabs
MACHINES CAN SEE

STORING AND HANDLING BIOMETRIC DATA: DO'S AND DONT'S

DO'S

ADDRESS INSIDE THREATS

Protect your network and data from internal threats with governance decisions (i.e., who has access to the data), monitoring and oversight.

MONITOR EVOLVING REGULATIONS

Policy and regulations change all the time. Make sure your data governance evolves accordingly.

MANAGE VULNERABILITIES

Many successful hacks succeed because of known vulnerabilities. Mitigate data breaches by ensuring the applications on your network are patched and up to date.

DONT'S

OVERLOOK ETHICS

Avoid sharing biometrics data with companies that do not provide a clear ethics and privacy statement.

MISUSE DATA

Ensure you use facial recognition data for ethical uses that protect citizens rights and privacy.

visionlabs.ai

Facial recognition for better, safer interactions in the connected world