Data Security Best Practices Klozer.io

A practical guide for protecting customer data, access, and communications

This document is designed for customers, operators, and internal teams at Klozer.io. It outlines the controls, habits, and operating standards that help reduce the risk of data loss, unauthorised access, misuse, and exposure.

1. Purpose of this guide
• Protect personal data and business data handled through Klozer.io.
• Reduce security risk across accounts, devices, systems, and communications.
• Support a consistent approach to access control, monitoring, and incident response.
• Help customers operate their environments in a secure and responsible way.

2. Core security principles
• Collect only the data you need.
• Limit access to the smallest group of people who need it.
• Protect data in transit and at rest.
• Keep systems updated and patched.
• Monitor activity and investigate unusual behaviour quickly.
• Retain data only for as long as it is required.

3. Access control best practices
• Use unique user accounts for every staff member.
• Require strong passwords and multi factor authentication wherever possible.
• Remove access immediately when staff leave or change roles.
• Assign permissions based on job duties rather than convenience.
• Review user access on a regular schedule.

4. Password and authentication standards
• Use long, unique passwords that are not reused across services.
• Store passwords in a secure password manager.
• Enable multi factor authentication for admin, billing, and support accounts.
• Do not share account credentials through email, chat, or spreadsheets.
• Reset credentials immediately if they are exposed.

5. Device security
• Use supported operating systems and browsers.
• Install security updates as soon as practical.
• Lock devices when not in use.
• Use screen locks, full disk encryption, and endpoint protection.
• Avoid accessing sensitive systems from untrusted devices.

6. Network and connection security
• Connect to trusted networks whenever possible.
• Avoid public Wi Fi for sensitive administrative work.

• Use secure connections and encrypted services.
• Review firewall, VPN, and remote access settings on a regular basis.
• Restrict remote admin tools to authorised users only.

7. Data handling rules
• Store sensitive files only in approved systems.
• Do not export data unless there is a clear business reason.
• Delete duplicate copies when they are no longer needed.
• Use masking or redaction when full details are not required.
• Verify the recipient before sharing files or records.

8. Email, messaging, and file sharing
• Check addresses carefully before sending confidential information.
• Use secure file sharing tools with access controls and expiry settings.
• Avoid sending sensitive data in plain text when a safer channel exists.
• Use approved communication tools for client records and internal collaboration.
• Do not forward internal data to personal accounts.

9. Backups and recovery
• Keep backups of critical systems and data.
• Test restoration procedures on a regular schedule.
• Store backup copies separately from live systems where possible.
• Protect backup access with the same care as production access.
• Document recovery roles and escalation paths.

10. Logging and monitoring
• Record key events such as logins, permission changes, failed access attempts, and export activity.
• Review logs for suspicious patterns.
• Alert on unusual behaviour, such as repeated failed logins or access from unfamiliar locations.
• Keep monitoring active for systems that handle customer data.

11. Vendor and subprocessors
• Review the security posture of service providers before use.
• Use written agreements that define security and privacy responsibilities.
• Limit vendor access to only the data required for the service.
• Review vendors periodically and remove unused integrations.

12. Incident response
• Report suspected incidents as soon as they are found.
• Contain the issue, preserve evidence, and assess scope quickly.
• Change affected credentials and permissions without delay.
• Notify the right people based on the severity of the incident.
• Document what happened, what was affected, and what was fixed.

13. Staff training and awareness
• Train staff on phishing, password safety, social engineering, and data handling.
• Repeat training for new hires and refresh it at regular intervals.
• Use short reminders and incident lessons to reinforce good habits.
• Make reporting suspicious activity simple and fast.

14. Physical security
• Secure offices, desks, meeting rooms, and printed records.
• Shred or securely dispose of paper records that are no longer needed.
• Do not leave laptops, notes, or access cards unattended in public spaces.
• Restrict visitor access to sensitive areas.

15. Remote work practices
• Use approved devices and approved software.
• Keep work areas private when handling sensitive data.
• Avoid screen sharing sensitive information unless needed.
• Sign out of sessions when stepping away from a device.

16. Data retention and disposal
• Keep only the data required for the agreed purpose.
• Apply retention rules consistently across systems.
• Dispose of old records securely.
• Delete or anonymise information when it no longer has a business need.

17. Practical checklist
• Enable multi factor authentication on all important accounts.
• Review user access every month.
• Patch devices and applications quickly.
• Use a password manager.
• Back up critical data.
• Train staff regularly.
• Document incidents and remedial actions.

Security control summary

Area	What good looks like	Review cadence
Access	Each person has an individual account, strong authentication, and the least privilege needed.	Monthly
Devices	Systems are updated, encrypted, and protected with approved security tools.	Weekly
Backups	Backups are available, protected, and tested for restore success.	Quarterly
Logs	Security and admin activity can be reviewed and investigated quickly.	Weekly
Vendors	Only approved providers are used and access is limited to what is necessary.	Quarterly

Important note: This guide is for operational and educational use. It should be reviewed by qualified legal and security advisers before publication if you want it to serve as a formal policy document.