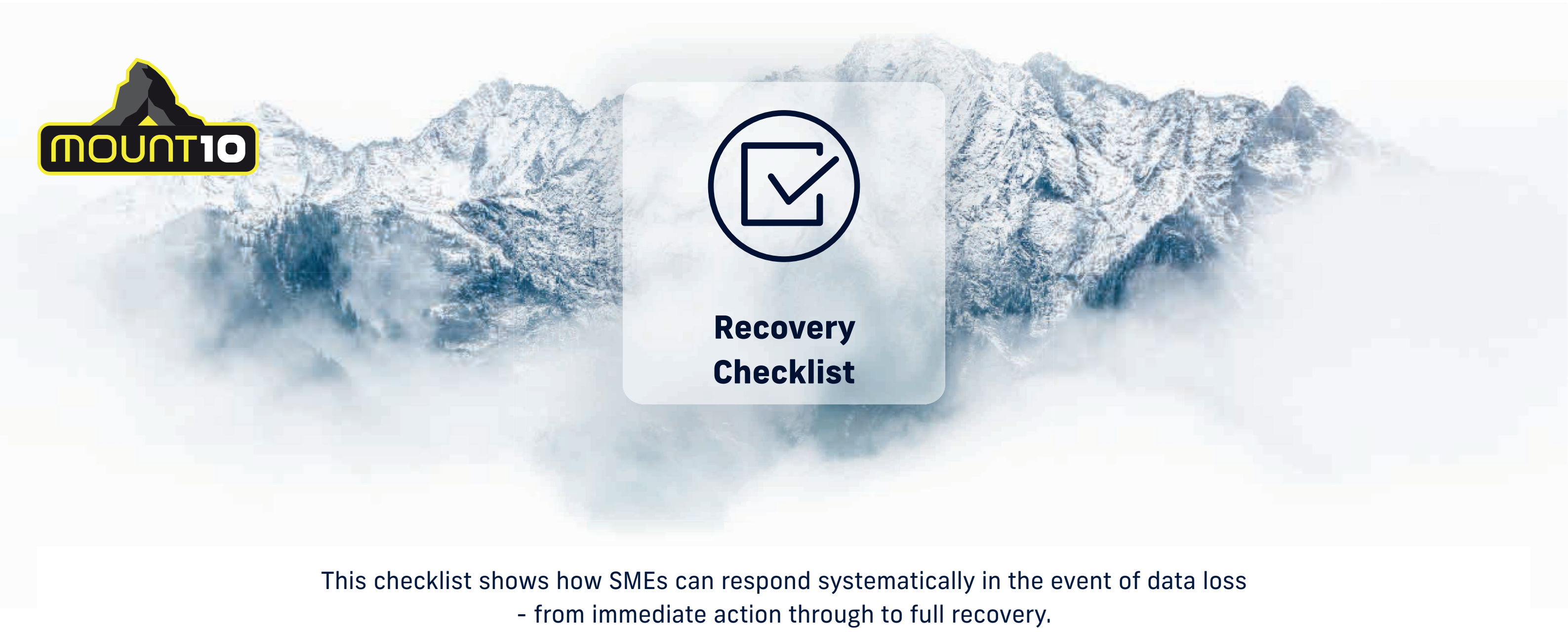


Recovery Checklist

This checklist shows how SMEs can respond systematically in the event of data loss - from immediate action through to full recovery.

1 - Immediate Actions - Stay Calm

- □ Inform the IT responsible person
- □ Disconnect affected devices from the network
- □ Document affected systems and data
- □ Do not attempt self-recovery or restoration without IT responsibility

2 - Analysis - Understand the Incident

- □ Review affected data (backups, local data, cloud services)
- □ Identify the cause (hardware failure, ransomware, human error)
- □ Record timelines and symptoms to assess the scope of the incident
- □ Determine which systems are critical to business operations

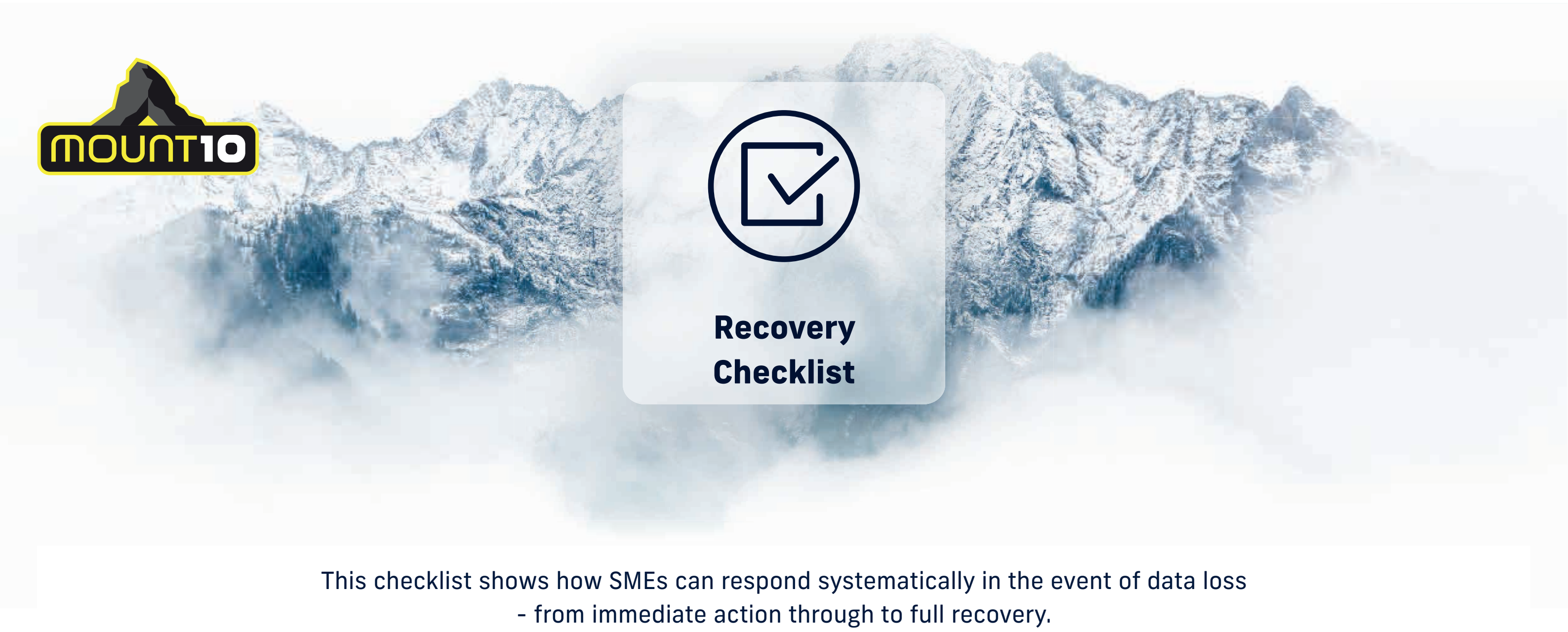
3 - Recovery - Use Backups

- □ Restore data from the last known good backup
- □ Verify that the backup is complete and intact
- □ Prioritize the restoration of critical systems
- □ Test data and systems after recovery before releasing them for production

4 - Communication - Internal and External

- □ Clearly inform employees about the incident and next steps
- □ If customers are affected: communicate factually and avoid causing panic
- □ Keep management continuously informed
- □ Use prepared text templates (e.g., MOUNT10 AI Prompt) to ensure consistent communication

The information provided here does not claim to be complete and does not constitute legally binding information.



Recovery Checklist

This checklist shows how SMEs can respond systematically in the event of data loss - from immediate action through to full recovery.

5 - Security Measures - Minimize Future Risks

- □ Review how the data loss occurred (security vulnerability, lack of isolation, etc.)
- □ Optimize the backup strategy (regular backups, immutable backups, separated systems)
- □ Provide regular data security training for employees
- □ Conduct regular recovery tests

6 - Post-Incident Review - Lessons Learned

- □ Document the incident (cause, duration, affected data, actions taken)
- □ Adjust internal processes and emergency plans
- □ Conduct an internal review to improve responsibilities and response times
- □ Update backup and IT emergency checklists

In Case of Data Theft

In the event of suspected or confirmed **data theft,** the relevant **authorities or the police** must be informed.
In Switzerland, reporting obligations apply under data protection law (e.g., notification to the FDPIC/EDÖB in the event of a data breach).

Involvement of External Specialists

For complex security incidents, engaging an **external incident response and digital forensics company** may be advisable.
External specialists support with: Root cause analysis and evidence preservation, damage assessment, legally compliant handling of the incident, system recovery and security hardening.

The information provided here does not claim to be complete and does not constitute legally binding information.