

Technical & Organisational Measures

Outecho · Sarajevo, Bosnia and Herzegovina · Applies to all client engagements

01 SCOPE

Outecho places senior software engineers into client engineering teams. Engineers work remotely from Sarajevo, in the client's own systems and tools. Outecho holds no primary copy of client production data; the measures below describe how access to client systems and any client personal data reached through them is controlled. They apply to every Outecho engineer, employed or contracted, for the full duration of an engagement.

02 MEASURES

Physical access	Engineering work is performed from the Outecho office in Sarajevo and from engineers' home offices. Office access is controlled by access cards, secured door locks and a monitored alarm system, and is restricted to Outecho personnel. Home working is permitted only on Outecho-issued or Outecho-managed devices. Engineers are instructed not to work on client data in public spaces, and not to connect from public Wi-Fi without a VPN.
Devices	All engineers work on Outecho-issued or Outecho-managed devices. Managed devices are enrolled in Outecho's device policy: full-disk encryption verified, automatic screen lock after 10 minutes of inactivity, active endpoint protection, and secure removal of client material at the end of an engagement. Operating systems are kept current with automatic security updates. No device outside this policy is used for client work. Outecho-issued devices are securely wiped before reissue on any personnel change. On managed devices, client material and access are removed and confirmed on engagement end.
System access	Named individual accounts only; shared credentials are not used. Multi-factor authentication is enforced on Outecho accounts and on any client system that supports it. Credentials are never shared by email or chat.
Data access	Engineers receive the minimum access required for their engagement. Access is granted by the client, reviewed at least quarterly and on every engagement change, and revoked on the last working day of the engagement. Outecho notifies the client on the same day so that client-side access can be closed in parallel. Each review is recorded with its date and outcome, and the record is available to the client on request.
Transfer	The client sets the terms for access to its systems. Where the client requires a VPN, a jump host, an IP allow-list or any other access method, Outecho and its engineers use that method and follow those terms. Absent client-specific requirements, connections are made over encrypted channels only. Client data is not copied to local storage except where necessary for the work, and never to personal cloud accounts or removable media.
Logging	Work is carried out in the client's own systems, whose logging and audit trails apply. Outecho separately records which engineer held which access, and when it was granted and revoked, and makes those records available to the client on request.
Instruction control	Engineers process client personal data only on the client's documented instructions. A named Outecho contact — the founder — is the escalation point for any question about the scope of an instruction, and notifies the client if an instruction appears to conflict with data protection law. Every engineer signs a confidentiality undertaking before any access is granted.

Availability	Outecho holds no primary copies of client production data; availability and backup of client systems remain with the client. Continuity of personnel is Outecho's responsibility: if an engineer is absent long-term or leaves, Outecho provides a vetted replacement, typically within 15 working days, with handover and onboarding at Outecho's cost.
Separation	Engineers work in a single client's systems per engagement. Full-time engagements are dedicated, so no shared working environment exists between clients. Outecho-side documentation and records are kept separately per client.
Personnel	Engineers are contracted by Outecho and sign confidentiality and intellectual property terms before starting work. A background check is performed before engagement, alongside reference calls with previous clients. All engineers complete an annual security and data protection briefing.

03 REVIEW AND CONTACT

These measures are reviewed at least annually and on any material change to Outecho's working practices. Questions, audit requests and security contact: benjamin@outecho.com. Outecho notifies the client of any personal data breach affecting client data within 24 hours of becoming aware of it.

v1.1 — September 2026, superseding v1.0 (August 2026). Material changes are versioned and dated, and the current version is available at any time on request.