cloudfactory

CloudFactory Security

When you need assurance that the data driving your AI models is safe and secure

Are you concerned about the security of your AI data?

CloudFactory takes data security very seriously and has made protecting client data a top priority. Our security options offer a layered approach to prevent unauthorized access and ensure compliance with regulatory, best practices, and client requirements.

Our Network Security is included in every client engagement, and establishes baseline security controls and features that protect our clients' data, regardless of where our teams complete the work. For clients with heightened requirements, our Endpoint Security upgrade enforces additional layers of workforce, IT, and network security.

Let's close the security gaps for AI data and models

People: Workforce security

When it comes to people, our workforce security ranks at the top. Client data will only be accessed by CloudFactory's employees, contractors, subcontractors, agents, or affiliates who adhere to our comprehensive security standards.

	NETWORK	ENDPOINT
Full background screening, training, and other evaluative measures conducted by CloudFactory, including personal interview and resume validation	✓	✓
Signed NDAs and remote work policy extending to all client work	✓	✓
Actively monitoring via desktop and webcam captures at random intervals to support security and performance monitoring	✓	✓
Team activity digitally monitored during all shifts by staff trained on data security guidelines	✓	✓
Industry-specific compliance training and adherence (e.g. HIPAA)	✓	✓

Technology: IT and network security

When it comes to technology, our IT and network security adhere to the strictest of guidelines. Client data will only be accessed through secured networks and devices adhering to our enterprise and data compliance standards.

	NETWORK	ENDPOINT
Antivirus installed on all workstations	✓	✓
Automatic Operating System Patching	✓	✓
Multi-factor Authentication (MFA) enforced on all user accounts	✓	✓
Access restricted by a secured virtual private network (VPN)	✓	✓
Ingress/egress firewall and IDS/IPS with deep packet inspection, advanced behavioral analysis, and traffic anomaly detection to determine zero day attacks	✓	✓

Technology: Workstations

All work is performed on CloudFactory provided workstations that are:

	NETWORK	ENDPOINT
Centrally managed to run antivirus software and actively scan for known and zero day threats		✓
Equipped with Vulnerability Management		✓
Customized Host Level Firewall Policies		✓
Equipped with full AES256 Host Level disk encryption using Bitlocker and managed through Endpoint protection		✓
Use Application Control to prevent launch and execution of certain applications		✓
Use Device Based Authentication that restricts remote access based on specific certificates		✓
Equipped with hardware and software that completely restrict the physical and non-physical removal of data		✓

Ready to protect your AI data and models to their full potential?

At CloudFactory, “we respect data” is one of our core principles. Our security commitment is integral to every solution we provide. Your data privacy and security are in trusted hands.

Learn more: https://www.cloudfactory.com/data-security