drivve | dm Cloud

Security Checklist

Physical Environment

- **Secure Areas** – IT facilities supporting critical or sensitive business activities are located within secure areas. Photo id validated and retained at building reception for each individual entry.
- **Physical Security Perimeter** – Strategically located barriers around defined perimeters provide physical security protection throughout the facility where sensitive business activities occur.
- **Physical Entry Controls** – Only authorized personnel can gain access to secure areas. Swipe-card access and/or biometric validation on initial entry to equipment rooms. Separate key access to each equipment rack where server hardware is stored.
- **Security of Data Centers and Computer Rooms** – Physical security for data centers and computer rooms is established that is commensurate with possible threats.
- **Isolated Delivery and Loading Areas** – The data center and computer room delivery and loading areas are isolated to reduce the opportunity for unauthorized access.
- **Equipment Location and Protection** – Equipment is located to reduce risks of environmental hazards and unauthorized access.
- **Power Supplies** – Electronic equipment is protected from power failures and other electrical anomalies.
- **Cabling Security** – All power and telecommunications cabling is protected from interception or damage.
- **Equipment Maintenance** – Procedures are established to correctly maintain IT equipment to ensure its continued availability and integrity.
- **Separation of Development and Operational Facilities** – Development and operational facilities are segregated to reduce the risk of accidental changes or unauthorized access to production software and business data.
- **Environmental Monitoring** – Host computer environments, including temperature, humidity, and power-supply quality, are monitored to identify conditions that might adversely affect the operation of computer equipment and to facilitate corrective action.
- **Media Handling and Security** – Computer media is controlled and physically protected to prevent damage to assets and interruptions to business activities.
- **System Planning and Acceptance** – Advance capacity planning and preparation ensures the proper availability of adequate capacity and resources as customer demands grow.
- **Capacity Planning** – Capacity requirements are monitored, and future requirements projected, to reduce the risk of system overload.

Network Management

- **Protection from Malicious Software** – Precautions are taken to prevent and detect the introduction of malicious software to safeguard the integrity of software and data.
- **Virus Controls** – Virus detection and prevention measures and appropriate user-awareness procedures have been implemented.
- **Network Monitoring** – 24/7/365 security monitoring of our network. Security of computer networks are monitored 24/7/365 and managed to safeguard information and to protect the supporting infrastructure.
- **Network Security Controls** – Appropriate controls ensure the security of data in networks and the protection of connected services from unauthorized access.

Electronic File Access

- **256-Bit Encryption** – Data stored on the file server is encrypted using the maximum encryption available, 256-bit AES encryption and SSL encryption for secure transfer of data.
- **Secured Socket Layer** – All communication is delivered over an industry-standard 128-bit encrypted SSL.
- **Access Controls** – User access to files is strictly granted on permissions basis, which administrators can easily change.

Policies and Procedures

- **Data Handling Procedures** – Procedures exist for handling sensitive data to protect such data from unauthorized disclosure or misuse both when on-site or in transit.
- **Clear Desk Policy** – A clear desk policy is enforced for sensitive material to reduce risks of unauthorized access, loss, or damage outside normal working hours.
- **Removal of Property** – Personnel are required to have documented management authorization to take equipment, data, or software off-site.
- **Operational Procedures and Responsibilities** – Responsibilities and procedures are established for the management and operation of all computers and networks.
- **Documented Operating Procedures** – Operating procedures are clearly documented for all operational computer systems to ensure their correct, secure operation.
- **Incident Management Procedures** – Incident management responsibilities and procedures are in place to ensure a quick, effective, orderly response to security incidents.
- **Operational Change Control** – Documented procedures are established for controlling changes to IT facilities and systems to ensure satisfactory control of all changes to equipment.
- **Data Backup** – Documented procedures are established for taking regular backup copies of essential business data and software to ensure that it can be recovered following a computer disaster or media failure.
- **Operator Logs** – Routine procedures are established for taking backup copies of data, logging events and faults, and where appropriate, monitoring the equipment environment.
- **Management of Removable Computer Media** – Procedures exist for the management of removable computer media such as tapes, disks, cassettes, and printed reports.
- **Fault Logging** – Procedures exist for logging faults reported by users regarding problems with computer or communications systems, and for reporting and taking corrective action.
- **System Acceptance** – Acceptance criteria for new systems are established and tested prior to customer rollout.
- **Vulnerability Testing** – Procedures exist to test for all OWASP categories of vulnerabilities on an ongoing basis.

Contact

For full worldwide locations visit www.drivve.com/contact

Drivve

Web | **www.drivve.com**

Email | **info@drivve.com**