empanel
ONLINE

Data Security & Continuity

Corporate Overview

Purpose

IMPORTANCE OF DATA AND DATA SYSTEMS

EMpanel Online is critically dependent on data and data systems. If important data were disclosed to inappropriate persons, the company could suffer serious losses. The good reputation that EMpanel Online enjoys is also directly linked with the way that it manages both data and data systems. For these and other important business reasons, our Executive Team has initiated and continues to support a data security effort. One part of that effort is definition of these data security policies.

ORGANIZATIONAL ACCOUNTABILITY

To be effective, data security must be a comprehensive effort, involving the participation and support of every EMpanel Online worker who deals with data and data systems. This policy statement clarifies the responsibilities of users and the steps they must take to help protect EMpanel Online's data and data systems. This document describes ways to prevent and respond to a variety of threats to data and data systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Scope

INVOLVED PERSONS

Every worker at EMpanel Online must comply with the data security policies found in this and related data security documents. Workers who deliberately violate this and other data security policy statements will be subject to disciplinary action up to and including termination.

INVOLVED SYSTEMS

This policy applies to all computer and network systems owned by or administered by EMpanel Online. This policy applies to all operating systems, computer sizes, and application systems. The policy covers only data handled by computers and networks.

Access Control

NEED TO KNOW

Access to data in the possession of, or under the control of EMpanel Online must be provided based on the need to know. Data must be disclosed only to people who have a legitimate business need for the data. At the same time, workers must not withhold access to data when the Owner of the data instructs that it be shared. To implement the need-to-know concept, EMpanel Online has adopted an access request and Owner approval process. Workers must not attempt to access sensitive data unless the relevant Owner has granted them access rights. When a worker changes job duties, including termination, transfer, promotion and leave of absence, his or her supervisor must immediately notify the Executive Team. The privileges granted to all workers must be periodically reviewed by data Owners and Custodians to ensure that only those with a current need to know presently have access.

USER IDs & PASSWORDS

To implement the need-to-know process, EMpanel Online requires that each worker accessing multi-user data systems have a unique user ID and a private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each worker is personally responsible for the usage of his or her user ID and password.

ANONYMOUS USER IDs

Users are prohibited from logging into any EMpanel Online system or network anonymously. Anonymous access might, for example, involve use of “guest” user IDs. When users employ system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on employing user IDs that clearly indicated their identities.

PASSWORDS CONTRAINTS

Passwords must be at least 10 characters long and include a mix of upper and lower-case letters, numbers, and special characters. Passwords must be changed every 90 days or at more frequent intervals. Whenever a worker suspects that a password has become known to another person, that password must immediately be changed.

PASSWORD STORAGE

Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down in some readily-decipherable form and left in a place where unauthorized persons might discover them.

SHARING PASSWORDS

Although user IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. System administrators and other technical data systems staff must never ask a worker to reveal their personal password. The only time when a password should be known by another is when it is issued. These temporary passwords must be changed the first time that the authorized user accesses the system. If a user believes that his or her user ID and password are being used by someone else, the user must immediately notify the system administrator.

Physical Security

DATA ACCESSIBILITY

Access to every EMpanel Online work area containing sensitive data must be physically restricted to those people with a need to know. When not in use, sensitive data must always be protected from unauthorized disclosure.

THEFT PROTECTION

Local area network servers and other multi-user systems must be placed in locked cabinets, locked closets, or locked computer rooms.

Network Security

INTERNAL NETWORK CONNECTIONS

All EMpanel Online computers that store sensitive data, and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Executive Team. Regardless of the network connections, all stand-alone computers handling sensitive data must also employ an approved password-based access control system.

EXTERNAL NETWORK CONNECTIONS (VPN)

All in-bound session connections to EMpanel Online computers from external networks must be utilize our encrypted Virtual Private Network (VPN). All requests for external access to internal EMpanel Online resources are reviewed by the Executive Team prior to granting VPN access.

NETWORK CHANGES

EMpanel Online adheres to a strict change control process for all network devices. Network device configurations are automatically backed up and continually monitored for changes. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of data, and other problems. This process applies not only to workers but also to vendor personnel.

Business Continuity

CLOUD-BASED RESOURCES

EMpanel Online utilizes a mixture of both public and private cloud offerings hosted in geographically disperse locations to minimize risk of outages from a single system or location.

SERVER VIRTUALIZATION

EMpanel Online heavily leverages server virtualization to reduce risk of hardware failure. Virtualization greatly increases disaster recovery options and provides a great deal of flexibility to meet business needs.

APPLICATION RESILIENCY

Whenever possible, EMpanel Online designs and employs systems that utilize multiple servers in load balanced clusters to ensure maximum performance and uptime.

BACKUP AND RECOVERY

All production systems at EMpanel Online are automatically backed up. Backup methodology will vary according to hosting platform and system function. In extreme cases, applications can be recovered to alternate EMpanel Online hosting facilities.

FORMAL CHANGE CONTROL

All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. This policy applies to servers running production systems and larger multi-user systems.

SYSTEMS DEVELOPMENT CONVENTIONS

All production software development and software maintenance activities performed by in-house staff must adhere to EMpanel Online policies, standards, procedures, and other systems development conventions. These conventions include the proper testing, training, and documentation.

PERSONAL BACKUP

Personal computer users must regularly back up the data on their personal computers, or ensure that someone else is doing this for them. For multi-user computer and communication systems, a system administrator is responsible for making periodic backups. An encrypted file sharing service (like Egnyte) is the recommended backup application for EMpanel Online PC users.

Internet and Computer Use

INTERNET ACCESS

Workers are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of a worker's supervisor.

EMAIL

Every EMpanel Online worker who uses computers in the course of their regular job duties will be granted an Internet electronic mail address and related privileges. All EMpanel Online business communications sent by electronic mail must be sent and received using this company electronic mail address. A personal Internet service provider electronic mail account or any other electronic mail address must not be used for EMpanel Online business unless a worker obtains management approval. All EMpanel Online workers must refrain from sending credit card numbers, passwords, or other sensitive data that might be intercepted.

VIRUS SCREENING

All personal computer users must keep the current versions of approved virus screening. Users must not abort automatic software processes that update virus signatures. Virus screening software must be used to scan all software and data files coming from either third parties or other EMpanel Online groups. This scanning must take place before new data files are opened and before new software is executed. Workers must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

SOFTWARE SERVICES

EMpanel Online computers and networks must not run software that comes from sources other than other EMpanel Online departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors.

ADEQUATE LICENSES

EMpanel Online management must make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for business activities.

UNAUTHORIZED COPYING

Users must not copy software provided by EMpanel Online to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from their supervisor. Ordinary backup copies are an authorized exception to this policy.

User Rights and Expectations

RIGHT TO SEARCH AND MONITOR

EMpanel Online management reserves the right to monitor, inspect, or search at any time all EMpanel Online data systems. This examination may take place with or without the consent, presence, or knowledge the involved workers. The data systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voice mail files, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature must be conducted after the approval of the Executive Team has been obtained. Because EMpanel Online computers and networks are provided for business purposes only, workers must have no expectation of privacy associated with the data they store in or send through these data systems. EMpanel Online management retains the right to remove from its data systems any material it views as offensive or potentially illegal.

PERSONAL USE

EMpanel Online data systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, and does not preempt any business activity.

SECURITY COMPROMISE TOOLS

Unless specifically authorized by the Executive Team, EMpanel Online workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise data systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Without this type of approval, workers are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

PROHIBITED ACTIVITIES

Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the VP of Operations. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of EMpanel Online internal policy.

Third-Party & Affiliate Data Handling

RELEASE OF DATA TO THIRD PARTIES

Unless it has specifically been designated as public, all EMpanel Online internal data must be protected from disclosure to third parties. Third parties may be given access to EMpanel Online internal data only when a demonstrable need-to-know exists, when an EMpanel Online non-disclosure agreement has been signed, and when such a disclosure has been expressly authorized by the relevant EMpanel Online data Owner. If sensitive data is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the data Owner and the Executive Team must be notified immediately.

THIRD-PARTY REQUESTS FOR EMPANEL ONLINE DATA

Unless a worker has been authorized by the data Owner to make public disclosures, all requests for data about EMpanel Online and its business must be referred to the Executive Team. Such requests include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing data about EMpanel Online products and services, nor does it pertain to customer technical support calls. If a worker is to receive sensitive data from third parties on behalf of EMpanel Online, this receipt must be preceded by the third-party signature on an EMpanel Online release form.

EXTERNAL DISCLOSURE OF SECURITY DATA

Data about security measures for EMpanel Online computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless approved by the VP of Operations or CIO.

Exceptions

The Data Security manager acknowledges that under rare circumstances, certain workers will need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by the Data Security manager.

Violations

EMpanel Online workers who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.