Dude Solutions Security Controls

Reducing Risks to Information Resources

Dude Solutions' Information Security policies and procedures reduce risks to information resources through implementation of controls designed to safeguard the security, availability and confidentiality of client data. Protecting all proprietary information relating to Dude Solutions and our clients is vital to the Dude Solutions mission.

Dude Solutions protects the privacy of client data using a layered defense-in-depth approach to information security. Our production network architecture prevents unauthorized access, as do Dude Solutions administrative access controls. Dude Solutions has adopted security policies and implemented company-wide information security training to protect the privacy of client data. By policy, Dude Solutions employees are prohibited from disclosing information obtained from clients to any other person or entity except in the performance of services for the client and only when the release of the information is authorized by the client.

All data transmissions over public networks are made using secure, encrypted connections. Dude Solutions applications utilize password-protected logins and user entitlement access control lists. Dude Solutions production servers are housed in a secure data center with restricted physical access. Industry standards such as ISO 27002 and NIST are used as best practices guidelines for Dude Solutions' information security program.

Sensitive Information Handling

Information Storage and Transmission	> Sensitive credentialing data, such as passwords, are salted/hashed using Password Based Key Derivative Function, also known as PBKDF2. > Databases containing user and company data such as usernames, addresses, emails and other personal information are encrypted using Transparent Data Encryption (TDE). TDE uses AES 256 encryption to encrypt the data at rest at the file level. Consequently, this sensitive data is also encrypted in backups. > IPSec VPN tunnels and TLS\SSL are used to transfer data between locations for disaster recovery and off-site backup.	> Dude Solutions safeguards all client information. Client information will only be disclosed to authorized personnel on a need-to-know basis. Dude Solutions shall ensure that appropriate administrative, technical and physical safeguards are established to ensure the security and confidentiality of this information is properly protected. At contract termination, client information can be exported and returned to client control.
Logging and Password Security	> User access log entries will be maintained, containing date, time, User ID, operation performed (created, updated, deleted) and source IP address. > If there is suspicion of inappropriate access, Dude Solutions can provide clients log entry records to assist in forensic analysis	> Logs will be kept for a minimum of 90 days > Logs will be kept in a secure area to prevent tampering > Passwords are not logged under any circumstances

Network Security

FIREWALLS

Dude Solutions uses a two-tiered firewall system that secures the environment from internet threats. The tier one firewalls filter all traffic into and out of the Dude Solutions network. A second tier of internal firewalls creates a web facing DMZ and provides an additional layer of security for client data.

INTRUSION DETECTION

Dude Solutions uses a third-party managed security service (MSS) which provides firewall management, IDS/IPS and other security services. Dude Solutions' MSS actively monitors network traffic and takes appropriate/specified action when security events occur.

VULNERABILITY ASSESSMENTS

Dude Solutions performs weekly network and application security vulnerability assessment tests. The results are reviewed by Information Security and, as necessary, any change recommendations are made to the IT Infrastructure Team.

ANTIVIRUS

Dude Solutions uses Symantec Antivirus Enterprise Edition to protect its production servers. Servers on the network have updated antivirus definitions pushed to them on a daily basis.

MONITORING

Hundreds of parameters of various types, including hardware, network, operating system and applications are continuously polled and trended. If a monitor exceeds predefined thresholds, an escalation process is followed for notification of appropriate Dude Solutions personnel.

DDOS PROTECTION

One of the most damaging brute force attacks an online application can experience is called Distributed Denial of Service (DDoS). These attacks are created by sending an overwhelming amount of attack traffic to a site from many external, typically virus-infected, machines. DDoS attacks can create so many packets that the traffic simply overwhelms and shuts down the online site. Dude Solutions uses advanced DDoS protection to match the sophistication and scale of such threats and can mitigate DDoS attacks of all forms and sizes.

The data center is staffed 24 hours a day, 365 days a year by trained staff and third-party security guards. The data center receives an annual SSAE 16 type II certification. Entry into the data center is restricted by proximity cards, access codes and biometric hand scanners. Facility security is managed centrally through a global facility management system. Video surveillance and stringent data center escort requirements protect server access.

Physical Security

Dude Solutions' Information Security Officer and Director of Facilities are responsible for the physical security of Dude Solutions' office premises. Dude Solutions' data center provider is responsible for the physical security of Dude Solutions' production servers housed at its data center, where client data is stored.

The data center is staffed 24 hours a day, 365 days a year by trained staff and security guards. The data center receives an annual SSAE 16 type II certification. Entry into the data center is restricted by proximity cards, access codes and biometric hand scanners. Facility security is managed centrally through a global facility management system. Video surveillance and stringent data center escort requirements protect server access.

All service center personnel must pass a background check, be trained in security procedures, and complete a probationary period with the company before being cleared for data center work. Physical access is provided only to authorized personnel, including employees, clients and vendors. All access is recorded and monitored. Daily audits ensure compliance with these activities.

Video tapes are rotated nightly at midnight and stored in a media safe in a locked room which is off-limits to clients. Electronic facility access logs are maintained on a non-network connected machine in a locked cabinet and have an effectively indefinite retention. Paper visitation logs are archived monthly into a cabinet in a locked room. Clients are required to sign in and present government issued ID to verify that they are authorized for access to their equipment as determined by the site access control list for each client.

Equipment brought in or out is logged at that time, and the particular equipment to which access is needed is granted via keys held by the data center security. Visitors must be escorted at all times while within the data center facility.

Security Policies And Procedures

Dude Solutions' Information Security program supports our data privacy and security management. The corporate Information Security Officer (ISO) develops information security policies and technical standards. These high level policies are reviewed and approved by executive management.

Any significant violations will be reported up through the business management chain to the executive levels of the organization. In addition to maintaining written policies, Dude Solutions has instituted an annual security and privacy awareness training program. All new employees will also be required to complete the training.

Pursuant to our Information Sensitivity Policy, data is classified according to its sensitivity level; the type of data determines its sensitivity and the treatment it is accorded. Client data is accorded treatment at the highest sensitivity level.As a general rule, client data is never disposed of or destroyed; it is returned to clients upon request. In the event that it was maintained on hardware that was taken out of service, the retired device is physically destroyed.

V1_012018

ABOUT DUDE SOLUTIONS

Dude Solutions is a leading software-as-a-service (SaaS) provider of operations management solutions to education, government, healthcare, senior living, manufacturing and membership-based organizations. For nearly two decades, Dude Solutions has inspired clients to create better work and better lives. We combine innovative, user-friendly technology with the world's smartest operations engine, empowering operations leaders to transform the most important places in our lives. Today, more than 10,000 organizations use our award-winning software to manage maintenance, assets, energy, safety, IT, events and more. For more information, visit dudesolutions.com.