Security Policies Overview

Direct Affinity Europe understands today's organizations require an exceptionally high standard of security management and that the confidentiality, integrity and availability of our customers' data is vital to their business operations and our own success. We take that to heart with our holistic approach to security, while constantly monitoring and improving our application, systems, processes and people to meet the growing demands and challenges of the evolving threat landscape.

Organisational Security

Security Team Structure

The DAE Information Security function consists of two functions/teams: Information Security & Engineering Security. The Information Security team is responsible for governance, risk, compliance, second line of defense, ownership of the Information Security Management System and overall security program management. The Engineering Security team is responsible for vulnerability management, incident detection and response, appsec assurance, management of security tools, security architecture solutions and monitoring throughout multiple stages of our software development life cycle.

Security Policies

Direct Affinity Europe has an Information Security Management System (ISMS) aligned with the ISO 27001 framework that includes policies and procedures to allow a systematic approach to protecting company information and assets from internal and external threats, reducing risk levels. These policies are readily available to all employees and include governance and risk management, human resources security, security of systems and facilities,

operations management, incident management, business continuity management, monitoring and security testing and privacy.

The Information Security team is responsible for monitoring compliance with data security policies and procedures.

Direct Affinity Europe is working towards full ISO 27001 accreditation within 12 months.

Confidentiality Agreements

All Direct Affinity Europe partners and employees, upon joining the company and/ or during their employment period, as well as certain service providers, are required to sign a non-disclosure and confidentiality agreements, demonstrating their commitment to the company and its information security principles.

Privacy

Ensuring customers' data is used only in a manner consistent with their expectations is a responsibility we take very seriously. We back our privacy guidelines with layers of security to safeguard their data.

Human Resources Security

People connecting to the Direct Affinity Europe network are required to conduct themselves in a manner consistent with the company security policies. This includes responsibilities before, during and after employment with DAE.

Code of Conduct

Direct Affinity Europe Code of Conduct and Internal Regulation addresses the appropriate use of company management of information to which employees have access to during the execution of the work agreement with DAE. Those who violate the Code or DAE policies and procedures will be subject to sanctions established by the employment legislation in force, up to and including dismissal, depending on the seriousness of the violation.

Security Training and Awareness

Direct Affinity Europe holds an Awareness Program with several initiatives. All DAE employees undergo security training as part of the onboarding process and receive ongoing training awareness that reinforces the security principles and policies, as well as industry best practices and common pitfalls. The Information Security team also distributes company-wide security alerts on an as-needed basis as risks and threats arise.

Termination Processes

Direct Affinity Europe has established documented termination processes that define their responsibilities for collection of information assets and removal of access rights for users who leave the company.

Infrastructure Security

Cloud Security

Direct Affinity Europe monitors Microsoft Azure accounts for cloud infrastructure security risks, such as IAM keys, network access control lists and security groups. The Engineering Security teams work closely with Site Reliability Engineering teams at infrastructure partners to remediate or mitigate any cloud infrastructure configuration risks that are found in our Microsoft Azure environments.

Encryption

Encryption is an important part of Direct Affinity Europe security strategy, and it's used as best practices for data in transit and at rest. For data in transit, we use TLS 1.2 with an industry standard ECDHE-RSA-AES128-SHA256 cipher.

Password Requirements

Direct Affinity Europe security policy establishes requirements for password changes, reuse and complexity. DAE requires the use of screensavers that reactivate after a period of inactivity through the use of a password or whenever a user leaves a computer unattended. As a matter of policy, employees are not permitted to share credentials with anyone.

Authentication Requirements

Employees sign on to Direct Affinity Europe cloud-based components utilizing a user ID, a password and a token (two-factor authentication).

This can greatly reduce the risk of unauthorized access if a user's password is compromised. VPN and 2FA is required to access production infrastructure systems (where information resides).

Network Security

All Direct Affinity Europe wireless networks are secured with WPA2. DAE infrastructure is hosted in Microsoft Azure and uses Azure controls such as Network Access Control Lists (ACLs), Security Groups and Subnet segregation. We also have web application firewalls (WAFs), Host Intrusion Detection Systems (HIDS), DDoS protections and firewalls in place to protect our production network.

Endpoint Security

All Direct Affinity Europe issued laptops have full-drive encryption enabled on them, which are continuously monitored and enforced to ensure full compliance.

Access Control

Access to Direct Affinity Europe information and systems is granted only to the extent necessary to perform assigned job responsibilities. DAE uses role-based security architecture and the principle of least privilege. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists.

For all terminations, access is removed on the employee's last day. Access reviews are performed periodically.

Customer Data

When customers use Direct Affinity Europe, we have an obligation to protect their data—that is part of our DNA. So, we give our customers control of the data by letting them decide who in their organization has access to what and allowing them to assign specific permissions to specific roles.

All DAE employees are trained and understand how to securely handle customer data to protect their privacy and confidentiality. We also embrace all GDPR principles and assume our processor duties. For our GDPR customers, we provide a Data Processing Agreement.

Audit

Direct Affinity Europe has the responsibility to safeguard customer data, which requires full knowledge of the operations executed on it, when they were done and by whom. DAE has integrated audit functionality that includes content access, update, creation/deletion and permissions in order to comply with customer and prospect requirements as well as compliance and regulatory concerns.

Physical Security

Office Security

Although Direct Affinity Europe does not manage physical infrastructure or data centers, physical access controls are implemented in DAE offices that typically include coded door locks, card-reader or biometric access to facilities.

Data Centre Security

Direct Affinity Europe data centers are hosted and managed by Microsoft Azure. Physical access to all Azure data centers, collocations and facilities housing IT infrastructure components is restricted to authorized data center employees, vendors and contractors who require access in order to execute their jobs. Azure utilizes multi-factor authentication mechanisms for data center access, as well as additional security mechanisms to ensure that only authorized individuals enter an Azure data center. Microsoft Azure continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Microsoft's data center operations have been accredited under ISO 27001, SOC 1 and SOC 2/SSAE 16/ISAE 3402, PCI Level 1 and FISMA Moderate.

Security Operations

Vulnerability Management

The Engineering team continuously monitors Direct Affinity Europe environments for system vulnerabilities and performs scanning on a recurring basis in accordance with DAE policy, by using industry standard scanning technologies. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Once a vulnerability requiring remediation has been identified, it is logged, prioritized according to severity and assigned an owner. The Engineering team tracks such issues and follows up frequently until they can verify that the issues have been remediated.

Patching

Direct Affinity Europe has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches. This process includes steps to review proposed patches to determine the risk of applying or not applying patches based upon the security and availability impact of those systems, and any critical applications hosted on them. DAE continually reviews patches and updates as they are released to determine their criticalities.

Penetration Testing

Penetration testing is completed at least annually to measure the security posture of a target system or environment. The Engineering team uses an accepted industry standard penetration testing methodology. Penetration testing also includes network and application layer testing.

Change Control

The goal of Direct Affinity Europe change management process is to prevent unintended service disruptions and to maintain the integrity of services provided to customers. Therefore, all changes, before deployed to production, are reviewed, tested, approved and communicated. This is aligned with our Systems/Software Development Life Cycle (SDLC). SDLC also covers documentation requirements, development practices and quality assurance testing requirements.

Segregation of duties

Different areas of responsibilities are segregated to reduce opportunities for unauthorized or unintentional modification or the misuse of our infrastructure.

Asset Management

Direct Affinity Europe uses an asset management solution to manage all computer assets.

Monitoring

Direct Affinity Europe management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two.

Incident Management

Direct Affinity Europe has a rigorous incident management policy for security events that may affect the confidentiality, integrity or availability of systems or data.

This policy covers four stages of the life cycle: Detection, Triage, Containment and Post-Incident. Each phase defines the goals for that phase, some major guidelines and who is responsible for all actions. For example, Detection covers the sources for events and incidents; Triage covers what should be evaluated in this phase; and Containment covers incident handling, including information gathering, how to avoid spreading and conditions to close the incident. Post-incident includes the need to do a post-mortem of the incident and incorporate learning and controls. It also covers metrics associated with incidents and specific requirements regarding privacy incidents (aligned with GDPR, HIPAA and PCI). Additionally, it includes a severity matrix and incident classification (type of incident). For data breaches, DAE will notify customers of any breaches affecting their data with a maximum SLA of 72h.

Business Continuity

Direct Affinity Europe has a Business Continuity Management System (BCM) that includes a Business Continuity Plan (BCP) for critical business functions that are integrated and aligned with site-specific incident response plans, disaster recovery plans and crisis management plans.

The primary goal of the BCMS is to ensure organizational stability, as well as coordinate recovery of critical business functions in managing and supporting business recovery in the event of disruption or disaster. DAE ensures disaster recovery plans to be tested periodically.

Third Party Risk Management

Direct Affinity Europe evaluates new third-parties to ensure they meet our security, quality and privacy standards.

DAE ensures formal agreements with them including, if applicable, clear definition of responsibilities, information security incident management, clear communication channels and points of contact for security and privacy topics (including for security incidents).

DAE also conducts regular due diligence to ensure information security posture and commitment from third-parties has not degraded over time. These reviews can be performed using reports from audit firms, surveys, penetrations test results, etc.

Compliance & Accreditation

Direct Affinity Europe works with software providers and infrastructure partners who hold several certifications such as SOC2 Type II, SOC3, PCI-DSS Level 1, ISO27001, ISO22301, CSA Star Level 1 and Cyber Essentials (UK). DAE has implemented an Information Security framework and is working towards its own certifications

Our dedicated team works every day to ensure the proper measures are in place to keep data safe. In addition to closely monitoring our threats landscape, they also conduct regular audits of our system.

Summary

At Direct Affinity Europe, we take security seriously and work every day to improve and keep information protected. The protection of user data is a primary design consideration for all DAE infrastructure, applications and personnel operations. Protection of user data is an integral part of what we do.