Whitepaper

ForgeRock Security

ForgeRock, the leader in digital identity management, helps customers safely and simply access the connected world. We offer a complete IAM platform to help customers transform how they can build trusted relationships with people, services, and things. Customers can monetize these relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway and Canada.

This Security White Paper describes security controls and principles deployed by ForgeRock across the enterprise to protect its assets and those of its customers, in addition to the critical support services ForgeRock offers to its customers and the ForgeRock Identity Cloud offering that builds upon ForgeRock's industry-leading on-premise solutions.

Table of Contents

Copyright © 2020 ForgeRock, All Rights Reserved.

ForgeRock Enterprise Security Controls and Principles

ForgeRock has founded its technology and personnel on the three core principles of information security:

- **Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities, or processes;
- **Integrity:** The property of safeguarding the accuracy and completeness of information and such assets;
- **Availability:** The property of information is accessible and usable upon demand by only authorised entities.

To ensure the Confidentiality, Integrity, and Availability principles are properly implemented across the company, a mature Information Security Management System (ISMS) has been set up along with a set of detailed security policies that all ForgeRock Staff must follow.

Roles and Responsibilities

The ForgeRock Board of Directors has the overall responsibility to provide management direction and support for information security in accordance with the business requirements and relevant laws and regulations.

The Chief Information Security Officer (CISO) is the owner of ForgeRock ISMS and all security policies, with all changes to ISMS and security policies being reviewed and approved by the CISO. The CISO leads the Enterprise Security team to ensure ForgeRock's security practices conform to international standards and are validated by regular audits.

A senior executive leadership team forum called the Privacy and Security Governance Board (PSGB) reviews and authorizes initiatives to strengthen security and privacy within the organization where necessary as well as constantly monitor and review substantial changes of threats against ForgeRock information assets.

Risk Management

ForgeRock's entire approach to information security is based on risk management. All security and privacy-related risks are captured and risk assessments conducted on a regular basis by the Enterprise Security team and the relevant Subject Matter Experts (SMEs) in accordance with standard risk management frameworks such as International Organisation for Standardisation (ISO) 27005 and National Institute of Standards and Technology (NIST) 800-37. All major risks are reviewed by senior executive leadership via the PSGB and where appropriate at the Board of Directors level. All risks categorized at not meeting a given threshold for acceptance are mitigated to reduce them to acceptable level.

Control and Classification of Assets and Security Enforcement

All ForgeRock physical and digital assets are identified and classified according to security level and access controls such as Public, Internal, and Confidential for documents and Sandbox, Pre Production, and Production for information systems and virtual assets with different levels of access control and security policies implemented against each level.

All physical assets are electronically tracked and managed by appropriate Asset Owners such as the Information Technology and Facilities teams. All virtual assets such as virtual machines, compute, storage and other virtual instances are tracked and managed both by the Enterprise Security team and by their business unit Asset Owner using the same cloud management and security control platform.

Only approved and secure builds are deployed both for physical and for digital production assets.

Onboarding of Staff Prior and Upon Employment

ForgeRock takes the security of its data and that of its clients and customers seriously and ensures that only vetted personnel are given access to ForgeRock resources.

Background Checks

All ForgeRock contractors and employees undergo background checks prior to being engaged or employed by ForgeRock in accordance with local laws and industry best practices such as British Standard 7858.

Copyright © 2020 ForgeRock, All Rights Reserved.

Confidentiality and Non-Disclosure Agreements

Confidentiality or other types of Non-Disclosure Agreements (NDAs) are signed by all employees, contractors, and others who have a need to access sensitive or internal information.

Acceptance of Applicable Policies and Agreements

All ForgeRock Staff read and accept all relevant security and privacy and other local and global obligations and expectations as part of the onboarding process such the ones spelled out in Acceptable Use Policy and other security policies as well as in Employee Handbooks.

Security and Privacy Awareness Training

All ForgeRock Staff undergo information security awareness and privacy awareness training as part of the onboarding process. All existing ForgeRock Staff undergo the latest security and privacy awareness training on an annual basis.

During Employment

ForgeRock Staff are required to review and accept all relevant security and privacy requirements as updated in existing ISMS and security policies. Staff undergo additional security or business-relevant training as part of the latest threats and risk assessments and as part of continuous improvement across the organisation. Breaches of the ISMS and any other ForgeRock guidelines result in disciplinary measures.

Termination or Change of Employment

Upon termination or conclusion of employment all physical and digital assets are handed in to the appropriate Asset Owners or System Administrators in accordance with set procedures. All access rights are revoked upon termination or organisational change where such access is no longer required. All ForgeRock Staff are notified of termination or change status in accordance with procedures set out by ForgeRock Human Resources (HR) team.

Physical Security

ForgeRock does not operate any Data Centres and relies on leading Cloud providers to maintain its infrastructure and services. ForgeRock does maintain good physical security practices for all of ForgeRock-managed offices via the following controls:

- All Information Technology (IT) equipment and all other equipment that require protection is stored in secure physical areas with badged access limited to authorised personnel only;
- IT equipment classified as “high” risk following risk assessment is protected against environmental threats (fires, flooding, temperature, variations, etc.).
- Information classified as “Confidential” is never stored on portable computer equipment. Should it be necessary to store this information on portable equipment, the information will be password protected and encrypted in compliance with the Enterprise Security guidelines;
- All ForgeRock Staff wear visible badges indicating their names and staff access levels;
- All office entries and exits are controlled by these access badges, with entries and exits logged by the door control system;
- All external doors and windows are locked upon termination of each working day;
- Alarms are set for all appropriate offices upon termination of each working day;
- Video surveillance is in use for offices where additional security is warranted and in accordance with local regulations;
- Maintenance workers and technicians are provided access after proper identification and authorisation;
- Visitors are signed in and signed out, given temporary visible guest cards during their visit, and are escorted by appropriate ForgeRock Staff for the duration of their visit.

Change Management and Operations Management

All ForgeRock System Administrators in charge of IT systems and services follow the principles set out in ForgeRock ISMS and related policies such as the Change Management Policy to ensure that:

- All proposed major changes are communicated to all relevant stakeholders;
- The Enterprise Security team is always one of the stakeholders. Requirements for information security are taken into consideration when designing, testing, implementing and upgrading IT systems, as well as during system changes;

Copyright © 2020 ForgeRock, All Rights Reserved.

- All major changes are documented and reviewed and authorized by senior management to ensure the changes are desirable, do not conflict with other proposed changes, and no significant issues have been raised by other stakeholders;
- All major changes are tested prior to deployment;
- Rollback plans or emergency procedures are created to revert changes if necessary;
- Operational procedures are documented and all technical staff are trained in their duties and responsibilities;
- Duties and responsibilities are separated for all systems, services, and applications in a manner reducing the possibility of unauthorised or unintended abuse of ForgeRock assets;
- Development, testing, and maintenance are separated from operations to reduce the risk of unauthorised access or changes, and to reduce the risk of error conditions.

Mobile Device Management, Endpoint Threat Management and Malware

All ForgeRock-issued devices have Mobile Device Management (MDM) to enable IT to deploy system critical patches, security updates, and any other security remote maintenance or protection to these devices. All devices with MDM are encrypted with the strongest level of encryption provided by the manufacturer and all data on those devices can be immediately locked or wiped remotely by MDM System Administrators upon instruction from the Enterprise Security team. If temporary exclusion to having MDM deployed is authorised by senior executive management for specific business reasons, such cases are documented and managed as risks by the Enterprise Security team.

All ForgeRock-issued devices have Endpoint Threat Management and Malware Protection deployed with live alerting, monitoring, and protection against the latest malware threats. The Enterprise Security team sets out the strategy and tactical deployment and implementation of Endpoint Threat Management solutions.

Installation of Software and Equipment Restrictions

Technical controls are deployed to prevent the installation of software or configuration changes to ForgeRock-issued devices, systems, and services.

Management of Storage and Removable Media

There is limited need for any kind of removable media, as ForgeRock generally relies on Cloud storage and applications. In most cases technical controls are in place to prevent the use of removable media by ForgeRock Staff. Where such controls are not technically possible or not business-necessary, ForgeRock relies on its Endpoint Threat Management solutions to assure security and prevent data exfiltration.

Network Administration

ForgeRock internal networks are protected by restricted access to only those personnel that require access to maintain and manage those networks, the use of strong credentials, and the use of Multi-Factor Authentication (MFA). Access is granted to only those ForgeRock Staff that require it for business duties and only to the services they are authorised to access. Access to privileged accounts and sensitive areas is restricted, with technical controls in place to prevent users from accessing unauthorised information. All access to ForgeRock networks is logged.

Exchange of Information and Use of Encryption

ForgeRock has technical controls and procedures for protecting exchange of information with third parties and information transfer, including contractual obligations. Storage and transfer of sensitive information is conducted via industry standard encrypted communication channels and storage methods. Information exchanged across public networks is protected against fraud, contractual discrepancies, unauthorised change or access by technical controls and proper secure implementation and deployment of systems, services, and applications.

Copyright © 2020 ForgeRock, All Rights Reserved.

Monitoring of System Access and Usage

Where permissible by law, access and use of ForgeRock IT systems is logged, analysed and monitored to detect unauthorised information processing activities with usage and decisions traceable to a specific entity.

All substantial disruptions and irregularities of system operations are documented, along with potential causes of the errors. All security incidents are logged for all essential systems. System clocks are synchronized to the correct time to allow for accurate security monitoring and investigation. Chain of custody procedures are established to preserve security incident evidence for sharing with government entities or litigation.

Access Control and Password Management

Access control and password requirements are regularly reviewed by Enterprise Security and all ForgeRock Staff are trained and made aware of the requirements that are applicable to their roles. Passwords and other credential secrets are rotated regularly according to business risks and require standard complexity and other similar best practices controls.

All users accessing ForgeRock systems, services, and applications are uniquely authenticated using strong credentials or other means as described in the ForgeRock Access Control and Password Management Policy and other ISMS policies. ForgeRock staff are trained and instructed to keep their passwords confidential and to use unique passwords for each service, system, or device where applicable.

Access rights, including accompanying privileges, are authorised by senior management according to business role and function. All access is granted on a "need to know" basis, and regulated according to role.

Mobile Equipment and Remote Workspace

Where needed and approved ForgeRock allows remote access to systems, services, and applications. Most of its infrastructure and underlying services run on top of leading Cloud Platforms. However, such remote access is restricted according to the sensitivity and security or privacy risk of the data or its systems, and where necessary additional controls such as MFA, Virtual Private Network (VPN), Remote Access Solution (RAS), or use of additional credentials.

Cryptographic Controls

All technical systems, services, and applications are deployed according to the latest cryptographic controls and guidelines provided by the Enterprise Security teams.

Secure Development Practices

All development projects at ForgeRock, including on-premising software products and coding patches, support services running on public Cloud infrastructure, and ForgeRock's own Digital Identity Cloud offerings follow the same Secure Development Lifecycle principles, founded on Microsoft's Security Development Lifecycle. All development of new products, tools, and services, and major changes to existing ones undergo a design review to ensure security and privacy by design requirements are incorporated into proposed development. In addition, all team members that are regularly involved in any system development undergo annual secure development training in coding or scripting languages that they work with as well as any other relevant training.

Once the design phase completes and coding begins, it follows stringent change controls procedures to ensure all changes are peer reviewed and only gets deployed to production once authorised and all system acceptance testing and security testing is successfully completed. Code is tested via static code analysis, dynamic code analysis, use case testing, internal penetration testing by internal security engineers, and in case of a major new product release or product update and external penetration testing as well. In addition, all third-party (open source) software is analysed and scanned for vulnerabilities before integration. Every security issue and vulnerability found during testing is triaged and addressed if considered high enough on the severity scale, such as Common Vulnerability Scoring System (CVSS).

Once the above tests are completed the code moves on to release testing where it is simulated to be deployed to production environments and validated that the new code behaves as expected and does not degrade or disrupt existing system(s). No production or customer data is ever used for any portion of code testing or release testing. Once release testing is successfully completed the code moves to production.

Copyright © 2020 ForgeRock, All Rights Reserved.

Incident Management

ForgeRock Enterprise Security team has established and regularly reviews and tests incident management plans and procedures to respond to security incidents, including having contracts with appropriate third-party vendors to help with investigation or resolution of potential incidents. ForgeRock's incident management practice is founded on the principles of detection, containment, eradication, and recovery where once a potential incident is identified, it is first contained so that it does not spread to further systems or assets, then eradicated where all compromised systems are cleaned or rebuilt, and finally recovered so that all operations are fully brought back online as before. As soon as a security incident is suspected to have involved any compromise or access to customer or supplier data an incident notification process is started and maintained with all potentially affected parties until brought to a resolution. Once the incident response is completed a post-incident review takes place where actions or controls leading up to the incident are improved and further protections are deployed where warranted.

All breaches of security, along with the use of information systems contrary to routines, are treated as incidents. All Incidents are reviewed by the CISO and with the PSGB where appropriate.

Business Continuity, Backup, Capacity Planning, and Disaster Recovery

ForgeRock IT systems and services rely on leading Cloud vendors such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure to ensure business continuity across the enterprise. ForgeRock Staff and office locations are spread out geographically with the capability of deploying a fully remote workforce such as during the COVID-19 pandemic to ensure no parts of ForgeRock business are rendered unavailable in an emergency.

Capacity planning is built into all of ForgeRock services with Cloud vendor scaling. ForgeRock uses license tracking and the cloud management security platform tool to keep track of assets and existing loads on services. Strong contractual agreements and Service Level Agreements (SLAs) with Cloud vendors allow for guaranteed uptime of ForgeRock systems and services.

Vulnerability and Patch Management

ForgeRock systems, applications, and services manage patches and vulnerability updates via standard change management practices where such updates and patches are reviewed for criticality and tested for business impact where appropriate prior to deployment according to emergency or scheduled deployment periods depending on the severity of each patch and vulnerability.

Penetration Testing and Vulnerability Scanning

ForgeRock deploys automated vulnerability scanning of all production and Internet facing systems on a regular basis. All new systems and services are scanned prior to being deployed to production. Manual penetration testing both by internal security engineers and external penetration vendors is performed on new major systems and products or major changes to existing systems, services, and products.

Supplier and Third-Party Management

ForgeRock follows the same risk-based approach to managing suppliers as to the rest of its information systems and services. Suppliers are reviewed on an annual basis and upon initial evaluation for contract where those that incur greater risk to the organization undergoing more detailed contractual reviews and negotiations and Third Party Risk Assessments to ensure ForgeRock has appropriate, Confidentiality, SLA, and security and privacy obligations written into Supplier contracts to ensure availability, integrity, and confidentiality of ForgeRock data held by these suppliers.

Compliance

ForgeRock regularly reviews all relevant legislations and existing contracts to ensure the organisation remains in compliance with current laws and contractual obligations. ForgeRock staff, customers, and suppliers are made aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following official authorised requests or court orders to do so. ForgeRock has a Privacy team lead by the CPC to ensure all personal information obtained and used in the provision of the business services at ForgeRock complies with applicable data protection regulations.

Copyright © 2020 ForgeRock, All Rights Reserved.

Controls and Audits

ForgeRock has a comprehensive internal auditing program to regularly review on at least an annual basis all of the applicable security and privacy controls as set out in the ISMS and related policies. This audit program is based on the ISO 27001 standard for which ForgeRock has obtained certification and undergoes continuous improvement as a result of previous internal and external audits and future certifications.

ForgeRock Identity Cloud

The ForgeRock Identity Cloud provides a comprehensive, flexible identity and access management platform run and operated by ForgeRock. ForgeRock secures, monitors, upgrades and runs the software while providing the flexibility and extensibility to satisfy some of the most complex identity and access management use cases in the industry. ForgeRock Identity cloud supports all major identity standards including OAuth 2.0, OIDC, SAML, CIBA as well as providing identity synchronization and storage. The ForgeRock Identity Cloud can be supplemented with the ForgeRock Identity Gateway™or ForgeRock Agents™ to provide policy enforcement and API management."

More information on Identity Cloud's features and benefits is available at https://www.forgerock.com/cloud.

More information on Identity Cloud's Security and Compliance is available at https://www.forgerock.com/resources/view/107430026/whitepaper/forgerock-identity-cloud-security-whitepaper.pdf.

Support Services Security

Forgrocks Support services are delivered via our 24/7 Secure Support Operations Center (SSOC)

This support service delivers customer support operations from our high security facilities which are certified to ISO27001 standards. all personnel utilise an isolated and hardened network and computer systems hardened to industry standards and certified to UK Government Cyber Essentials Plus standards including restrictions on hardware and software profiles as well as DLP technology to prevent data egress and Ingress monitoring to assure the security of data entering the facility.

Access to facilities is restricted only to our vetted support personnel and is monitored by 24/7/365 CCTV coverage.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com** or follow ForgeRock on social media.

Follow Us

ForgeRock

Copyright © 2020 ForgeRock, All Rights Reserved.