HackerRank

Security You Can Trust

INFORMATION SECURITY WHITEPAPER

Table of Contents

1. **Introduction**
2. **Reliability**
    a. Performance monitoring
    b. Quality by design
    c. Incident response
    d. Status transparency
    e. Scalable storage and backup
    f. Disaster recovery and business continuity
    g. Support
3. **Security**
    a. End-to-End data encryption
    b. Application vulnerability assessments
    c. Information security
    d. Physical security
    e. Organizational security
    f. Network security
    g. Classifying and inventorying data
    h. Change management
4. **Visibility and Control**
    a. Logging and monitoring
    b. Role-based access controls
    c. Single sign on and authentication
    d. HackerRank APIs
    e. Audit API
5. **Privacy and Compliance**
    a. ISO 27001
    b. GDPR
6. **Conclusion**

HackerRank: Security You Can Trust

1.0 Introduction

HackerRank is the best end-to-end technical recruiting platform for hiring developers. We power our platform with the most reliable and secure technology and processes to ensure your data is always protected. Your trust in us is of the utmost importance and we are committed to ensuring a safe and secure experience using HackerRank.

At HackerRank, our top priority is keeping your data secure. **Customer data stored in HackerRank is of nominal value and is limited to public and internal data classification with low risk/ sensitivity.** However, we are committed to providing the highest levels of security and controls to ensure the confidentiality, integrity, and availability of your data, applications, and infrastructure at all times.

Our comprehensive security program includes rigorous policies and procedures governing the reliability of our infrastructure; the security of data, applications, and network; visibility and access controls; and privacy and regulatory compliance. Read on to learn more about how we maintain enterprise-grade protection for our customers.

2.0 Reliability: HackerRank is reliable to the core.

HackerRank uses Amazon Web Services (AWS) as its sole hosting provider. The HackerRank application and services are built on a resilient, cloud-based architecture that delivers multiple levels of protection to safeguard data and files.

Built on industry-leading AWS infrastructure and hosted in AWS Virtual Private Cloud (VPC), HackerRank is designed for high availability with a tiered architecture across subregions and subnets. With the implementation of gateways, authorization mechanism, logical and secure routing of traffic and communications among tiers and the internet, HackerRank delivers optimal performance with redundancy and failover options around the world to ensure a highly available and resilient service. AWS can quickly respond to increases in user load, allowing us to provide reliable, predictable performance that scales as needed.

In addition, we ensure high availability and performance for the HackerRank platform by:

Performance monitoring: We constantly monitor key performance measures such as load times, search responsiveness, attachments, and data delivery.

Quality by design: Our rigorous quality assurance process includes testing with a small number of customers to quickly identify issues and fine tune quickly to ensure an optimal customer experience.

Incident response: Our teams adhere to a strict global incident response process with multiple levels of escalation designed to reduce the impact of incidents and shrink the amount of time it takes to resolve incidents.

Status transparency: Our service is supported by multiple, redundant data centers around the world that deliver 99.9% service availability. Our performance dashboard provides a constant view into operational uptime so that you can see how our system is performing, anytime, anywhere.

Scalable storage and backup: Through the Amazon Relational Database Service (RDS) we leverage Multi Availability Zones that are engineered for high availability and are highly reliable in the event of an infrastructure failure or natural disaster. In HackerRank, at least one generation of backup files is maintained on off-line data storage media wherever production computers are located. At least two recent and complete backups made on different dates containing critical HackerRank product records are always stored off-site.

Disaster Recovery and Business Continuity: AWS provides multiple geographic regions and availability zones, which allows HackerRank to remain resilient in the event of a failure, including natural disasters or system-wide failures. All data collected is contained within an AWS Virtual Private Cloud (VPC) that uses AWS Region us-east-1 (N. Virginia) as a primary location and AWS Region us-west-2 (Oregon) as the secondary disaster recovery location.

Support: HackerRank's comprehensive support site provides all the resources for users and administrators alike to get the most out of the HackerRank platform. Visit our support site for access to online training, tutorials, quick start guides and more, or submit a request to our expert support staff.

3.0 Security: We deliver enterprise grade protection.

At HackerRank, we are committed to providing the highest levels of security to ensure that your data, applications, and infrastructure remain safe.

The HackerRank platform is built on Amazon Web Services (AWS), a secure cloud services platform. On AWS, we have designed a multi-tiered architecture that offers enhanced security and avoids any single points of failure. Each tier has its own Access Control List (ACL) and rule set to restrict access and allow secure communications. Data is fully segregated and all access is done through certificate-based authentication. In addition, the AWS infrastructure is fully compliant with globally accepted security standards, including ISO 27001 and SOC 1/SOC 2/SSAE.

In addition to our secure architecture, we have implemented a wide range of security processes, procedures, and technologies designed to protect our customers, including:

End-to-end data encryption: HackerRank secures all customer data with end-to-end encryption. This includes:

- Encryption in transit: Encryption of all data in transit is done through FIPS-compliant TLS/SSL protocols via HTTPS. HackerRank uses the 2048 bit asymmetric key for the SSL/TLS handshake and the AES-256 bit or AES-128 bit key depending on the client browser. We use the SHA-256 cipher on the SSL/TLS session to ensure the integrity of the encrypted data. Our SSL Server Test vendor gives us an A+ grade for our SSL certificate.

- Encryption at rest: All data in our data store uses 256-bit AES encryption. HackerRank uses Amazon Relational Database Service (RDS), which supports encryption of data at rest. Amazon RDS-encrypted instances use the industry standard AES-256 encryption algorithm to encrypt data. Once encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. The encryption keys are stored in a separate Amazon Key Management System (KMS). Only specified users can access the KMS and the encryption keys are not persisted anywhere in the storage layer. This ensures that only the intended recipient can access the encrypted information.

Application vulnerability assessments: We engage third-party security experts to conduct independent internal and external network, system, and application vulnerability assessments.
These include automated and manual application security testing, SSL server tests, and continuous risk monitoring of all HackerRank properties and third-party applications. As an additional security layer, we implement the HackerOne Bug Bounty program, which tests applications for vulnerabilities.

Information security: HackerRank's information security management framework outlines how we protect your data. To minimize risk of data exposure, we restrict user access employing RBAC, SSH private keys, VPN with two-factor authentication and special access vetted by security team. Our software development cycle requires adherence to secure coding guidelines and we conduct source code scanning and analysis to detect security issues. We regularly review and update security policies, provide security training, and ensure compliance with security policies.

Physical security: HackerRank's production systems and customer data is housed in AWS data centers, which follow industry best practices for security and also comply with a wide range of industry standards and regulations. HackerRank's offices follow strict security procedures to maintain security, including managing visitors, monitoring building entrances, and employing CCTVs.

Organizational security: HackerRank employees are trained in information security processes and procedures as part of the onboarding process. All employees are required to take security and privacy training on an annual basis, which covers our information security policies, security best practices, and privacy protections. Employees with access to production and corporate environments are required to use SSH private keys to securely log in. To access systems remotely, employees must use a VPN with two-factor authentication.

Network Security: We have implemented multiple layers of defense and proactive security procedures such as perimeter defense, network security monitoring and intrusion detection systems to protect the quality and integrity of our network. Our security team ensures that server, firewall, and other security-related configurations are kept up-to-date with industry standards. We identify and mitigate risks via regular application, network, and other security testing, which is audited by our internal security team as well as third-party security specialists.

Classifying and inventorying data: HackerRank does not store Personally Identifiable Information (PII) in its systems. The customer data stored in HackerRank is of nominal value and is limited to public and internal data classification with low risk and sensitivity. For example, candidates that are invited by recruiters to take an assessment on the HackerRank platform need only submit an email address. All other data, such as test results and candidate reports are classified as low risk and sensitivity as these are a prospective employee information and not employee data. We review this data regularly to ensure it is correctly classified.

Change Management: Any changes to the HackerRank environment could impact our security posture. To minimize the risk of unintended consequences, our Engineering team has defined a formal change management policy to ensure that only authorized application changes are implemented into production systems. In addition, all changes go through quality assurance testing to ensure that security controls are in place.

4.0 Visibility and Control: Grant access only where and when users need it.

We offer a wide range of visibility and control features that enable your administrators to customize HackerRank for your organization's specific access control needs. The HackerRank dashboard provides deep visibility into the performance and availability of your environment.

Logging and monitoring: Our security team monitors all servers and devices in our environment and regularly reviews logs to track access and look for indications of suspicious or unauthorized activity.

Role-based access controls: Administrators can manage who has access to data and resources in HackerRank according to their role in the organization. The "Teams Management" section of HackerRank allows administrators to set up groups of users in order to simplify operations that involve multiple people and resources and assign permissions based on a user's duties.

Single sign-on and authentication: We streamline authentication by providing single sign-on (SSO) capabilities via our SSO partners or your preferred SAML 2.0-compliant solution. SAML allows for a seamless, single-sign-on experience between your internal web portal and HackerRank.

HackerRank APIs: We have a set of APIs that automate repetitive tasks such as test administration and fetching results. Customers can use our APIs to generate dashboards, integrate with their HR systems, or leverage our pre-built integrations with the most popular Applicant Tracking Systems.

Audit API: We have a set of APIs which can be used to retrieve audit logs of all actions taken by any user(s). Every change made to your Tests, Questions, Teams, Candidates and/or any other object is documented and accessible via this API.

5.0 Privacy and Compliance: We are committed to protecting your privacy.

HackerRank is committed to protecting your privacy and maintaining your trust. Our privacy program includes strict policies and procedures regarding access to and the use, disclosure, and transfer of customer data. We comply with the most widely accepted standards and regulations, validated by independent third-party audits, in order to help you meet your privacy obligations. Read our privacy policy to learn how we protect your information.

We comply with major global privacy standards, including:

ISO 27001: ISO 27001 is a globally recognized, standards-based approach to security that outlines requirements for an organization's Information Security Management System (ISMS). HackerRank is ISO27001-certified which reaffirms our commitment to security.

General Data Protection Regulation (GDPR): HackerRank has implemented numerous privacy and security practices in order to ensure we are fully compliant with GDPR and provide product functionality that enables our customers to remain compliant. Because we process candidates on behalf of our customers, we are considered a Data Processor and the customer organization is regarded as the Data Controller. As a Data Processor, all the candidate information we receive or collect is handled securely. We also have an incident response plan in place to address unforeseen incidents that may put personal information at risk, as mandated by GDPR. As required by GDPR, HackerRank has a data processing agreement (DPA) that incorporates all the GDPR clauses and ensures our compliance. Learn more about our GDPR compliance here**.**

6.0 Conclusion

At HackerRank, your security and privacy is our top priority. Our comprehensive security program is designed to deliver the highest levels of security and controls to ensure the confidentiality, integrity, and availability of your data, applications, and infrastructure at all times. Maintaining your trust in us is of utmost importance. If you have any questions or would like more information about our security processes and procedures, contact us at security@hackerrank.com.

About HackerRank

HackerRank is an end-to-end technical skills assessment platform that is the standard for assessing developer skills for over 1,100 companies across industries and around the world. By enabling technical recruiters and hiring managers to objectively evaluate talent at every stage of the recruiting process, HackerRank helps companies identify skilled developers faster, increase candidate quality, and recover valuable recruiting and engineering time. To learn more about HackerRank, visit HackerRank.com.