HackerRank

Information Security Policies

HackerRank has implemented the technical and organizational security measures outlined in the attached documents:

1. Information Security Policy: Acceptable Use of Assets Policy
2. Information Security Policy: AMI Policy
3. Information Security Policy: AWS Remote Access Policy
4. Information Security Policy: Backup and Restore Policy
5. Information Security Policy: Incident Reporting and Response Policy
6. Information Security Policy: Information Classification Policy
7. Information Security Policy: Password Management Policy
8. Information Security Policy: Security Group Management Policy

Information Security Policies

Acceptable Use of Assets Policy

Policy #	IS-01	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari K	Phone	

Table of Contents

3.0 PURPOSE

This policy defines the activities that are permissible when using any Interviewstreet computer and device.

4.0 SCOPE

This policy applies to all users of Interviewstreet information assets including but not limited to Interviewstreet employees and partners.

5.0 POLICY

User IDs and Passwords

Personal User IDs — Responsibility - Users must be responsible for all activity performed with their personal user IDs. They must not permit others to perform any activity withtheir user IDs, and they must not perform any activity with IDs belonging to other users.

Access Code Sharing - Interviewstreet computer accounts, user IDs, networkpasswords, voice mail box personal identification numbers, credit card numbers, and otheraccess codes must not be used by anyone other than the person to whom they were originally issued.

Script Files On Portable Computers, PDAs, And Smart Phones - Users must not store clear-text authentication credentials on portable computers, personal digital assistants, or smart phones, and must never set-up or employ script files that contain a stored version of a personal identification number (PIN), a password, or a user-ID which can be used togain access to a Interviewstreet information system. Likewise, these security parametersshould never be stored anywhere on these devices unless they are in encryptedform.

Typing Passwords When Others Are Watching - Workers must never type their passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

Password Structure - Workers must not employ any password structure orcharacteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences, personal details, or any part of speech.

Suspected Password Disclosure - Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

Password Proximity To Access Devices - Users must never write down or otherwise record a readable password and store it near the access device to which it pertains.

Passwords In Communications Software - Users must not store fixed passwords indial- up communications programs, email clients, or related data communications software at any time.

Electronic Messaging

Reasonable Personal Use Of Computer And Communications Systems - Interviewstreet allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use must beconsistent with conventional standards of ethical and polite conduct. For example, electronic mail must not be used to distribute or display messages or graphics which may be considered by some to be disruptive or offensive (such as sexual jokes orpornography).

Offensive Electronic Mail Messages - Workers are encouraged to respond directly tothe originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, workers must report the communications to theirmanager.

Sending Unsolicited Electronic Mail - Users must not send uninvited or unsolicited electronic mail (also known as spam) to a large number of recipients. This includes commercial advertisements, charitable solicitations, questionnaires/surveys, chain letters, and political statements. If you do send spam and the recipients contact theInterviewstreet mail system administrator with complaints, you will be subject to disciplinary action including loss of system privileges and termination.

Identity Misrepresentation - Workers must not misrepresent, obscure, suppress,or replace their own or another person's identity on any Interviewstreet electronic communications.

Electronic Mail System Usages - Workers must use Interviewstreet electronic mail systems primarily for business purposes, and any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for- profit outside business activity, and must not potentially embarrass Interviewstreet.

Permissible Uses Of Instant Messaging Facilities (IM) – Limited Use - Interviewstreet instant messaging (IM) facilities must be used for business purposes only. All Interviewstreet business related IM messages must be sent through the Interviewstreet IM system. Ifusers wish to send personal instant messages, they must use a consumer IM client to keep personal information out of the business IM system archive of all messages. The business IM system may be used for collaboration and coordination only. Contractually binding agreements, as well as sensitive information, must be sent through other communication channels.

Internet and Intranet

Third Party Web Based Services – Interviewstreet provides every worker with access to a set of web based services that support company operations. This includes, but is notlimited to, Google Apps, GitHub, and Amazon Web Services. Whenever possible, workersshould take full advantage of these services. All business related material should be storedon these services.

Forwarding Intranet Information - Workers must not forward information appearing onthe intranet, or services such as Google Drive or GitHub, to third parties without firstobtaining approval from the Interviewstreet information's Owner.

Internet Information Modifications - Users connecting to Interviewstreet systems through the Internet must not directly modify any Interviewstreetinformation.

Internet Discussion Groups - Users must not post to controversial discussion groups on the Internet or to any other controversial online public forums when using their Interviewstreet user IDs.

Personal Internet Message Disclaimers - Whenever a worker posts a message to an Internet discussion group, or another public information system, without prior approval from the Marketing Department, this message must be accompanied by words clearly indicating that the comments do not necessarily represent the official position of Interviewstreet.

Internet Product And Service Representations - Workers must not advertise,promote, present, or otherwise make statements about Interviewstreet products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Marketing Departments.

Uploading Software - Users must not upload software that has been licensed from a third party, or software that has been developed by Interviewstreet, to any service or server through the Internet unless authorization from the user's manager has first been obtained.

Personal Accounts - Workers who wish to make a statement in a public Internet forum about any topic that does not involve Interviewstreet business, or Interviewstreet business interests, must use their own personal accounts to submit such statements.

Personal Use Of Internet Resources From Remote Locations - Workers must not initiate connections to the Internet, or otherwise use Internet resources, from remote locations, if this activity goes though Interviewstreet systems and/or networks, and if this activity is personal in nature.

Personal Use Of Internet - Use of Interviewstreet information systems to access the Internet for personal purposes will not be tolerated and may be considered cause for disciplinary action up to and including termination. All users of the Internet should be aware that firewalls can create a detailed audit log reflecting transmissions, both in-bound and out- bound.

Internet Connection Approval - Workers must not establish any external network connections that could permit non-Interviewstreet users to gain access toInterviewstreet systems and information, unless prior approval of the Chief Technology Officer hasfirst been obtained.

Large Internet Downloads - Internet users must not use video streaming facilities, audio streaming facilities, or download large graphics files unless these transmissions are approved in advance by the user's manager.

Sensitive Information Not Accessed from Public Terminals - Employees must notuse public web terminals to access sensitive Interviewstreetinformation.

Unencrypted Personal Identifiers Sent Via Internet Prohibited - Workers mustnever transmit any personally identifiable information (such as social security numbers and birth dates) unencrypted over the Internet. This prohibition includes email, instantmessaging, chat rooms, and other communication systems.

Internal Systems

Involvement With Computer Viruses and Malware - Users must not intentionallywrite, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Interviewstreet computer or network.

Hacking Activities - Workers must not use Interviewstreet information systems toengage in hacking activities that include, but are not limited to: (a) gaining unauthorized accessto any other information systems, (b) damaging, altering, or disrupting the operations ofany other information systems, and (c) capturing or otherwise obtaining passwords,encryption keys, or any other access control mechanism that could permit unauthorizedaccess.

Circumventing Access Controls - Developers and other technically-oriented staffmust refrain from installing any code that circumvents the authorized access control mechanisms found in access control systems.

Testing Information System Controls - Workers must not test, or attempt to compromise internal controls unless this activity is specifically approved in advance, and in writing,by their manager.

Encryption Usage Aside From That In Browsers - Aside from the encryption that isbuilt into Internet browsers, users must not employ encryption of any sort when usingcomputer systems or networks unless these encryption systems have first been established and approved by their manager.

Incidental Personal Use Of Computer Communications Systems -Interviewstreet information systems are provided for, and must be used only for business purposes. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with employee productivity, and (c) does not preempt any business activity.
Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a personal lunch.

Prohibition Against All Forms Of Adult Content - All forms of adult content (pornography or what some would consider to be pornography) are prohibited on Interviewstreet computers and networks. This includes content obtained via web sites, emailattachments, and file sharing networks.

Software Duplication - Users must not copy software provided by Interviewstreet to any storage media, transfer such software to another computer, or disclose such softwareto outside parties without written permission from theirmanager.

Unauthorized Software And Data Copies - Interviewstreet strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If employees users make unauthorized copies of software, they are doing so on their own behalf, since all such copying is strictly forbidden by Interviewstreet. Likewise, Interviewstreet allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

Equipment

User Installation Of Software - Users must not install software on their personal computers, network servers, or other machines without receiving advance authorization to do so from a local information security coordinator.

Sharing A Personal Computer With Other People Prohibited - Workers must not share their personal computer, if it is used for Interviewstreet business, with any other person except for actives that support business objectives.

Unattended Active Sessions - If the computer system to which they are connected or which they are using contains sensitive information, users must not leave their personal computer unattended without logging out or invoking a password-protected screen saver.

Accepting Security Assistance From Outsiders - Users must not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by the Chief Technology Office. This means that users must not accept offers of free consulting services, must not download free security software via the Internet, and must not employ free security posture evaluation web pages, unless the specific provider of the assistance has been previously approved.

Personally-Owned Computer Systems - Workers must not bring their own computers, computer peripherals, or computer software into Interviewstreet facilities without prior authorization from their manager.

Games On Organization Computer Systems - Games may not be stored or used on any Interviewstreet computer systems.

Secret Information On Transportable Computers - Workers possessing a laptop, smart phone, or tablet containing confidential Interviewstreet information must not leave these devices unattended at any time unless the information contained therein is exclusively stored in encrypted form.

Transportable Computers On Airplanes - When traveling by air with a laptop, smart phone, or tablet containing sensitive Interviewstreet information, workers must not check these computers in airline luggage systems.

Lending Computers Containing Sensitive Information - A personal laptop, smart phone, tablet, or any other computing device used for business activities that contains sensitive information must not be lent to anyone.

Securing Information

Storing Mixed Classified Information - Interviewstreet workers must not store sensitive information with non-sensitive information in the same media container. This includes removable media and AWS services.

Storage Of Sensitive Information - Interviewstreet workers must not: 1) store private, confidential, or secret information on any type of removable media 2) use any web based services, other than those provided by Interviewstreet, to store confidential or secret information.

Disclosing Customer Business Information - Interviewstreet workers must not disclose to anyone outside Interviewstreet the nature of customer projects, customer business strategies, or customer business relationships.

Disclosure Of Third-Party Information - Interviewstreet workers must not disclose sensitive information that has been entrusted to it by third parties to other third parties unless the originator of the information has provided advance approval of the disclosure and the receiving party has signed an approved non-disclosure agreement.

Trade Secret Disclosure - Workers must diligently protect from unauthorized disclosure all Interviewstreet information specifically identified as trade secrets. Trade secrets must be identified as such prior to being disclosed to any workers.

Copying Sensitive Information - Making additional copies of, digital or through printing, of secret, confidential, or private information must not take place without the advance permission of the Information Owner.

Securing Sensitive Information - Workers in custody of Interviewstreet sensitive information, such as information classified as Confidential or Secret, must take appropriate steps to ensure that these materials are not available to unauthorized persons.

Downloading Sensitive Information Approval - Sensitive Interviewstreet information must not be downloaded from a multi-user system to a personal computer unless a clear business need exists and advance permission has been obtained.

Mobile Computer Alternatives - When away from Interviewstreet offices, mobile computer users must utilize either encryption software to protect the sensitive information when it is held in internal computer system storage, or employ some technique to physically secure removable media on which the sensitive information resides.

Record Destruction Schedule - Workers must not destroy Interviewstreet records unless these records appear on a list of records authorized for destruction.

Sensitive Information Retention For Destruction - Workers must not discard sensitive information in publicly-accessible trash containers. They must instead securely retain sensitive information until it can be shredded or destroyed with other approved methods.

Portable Computer Data Storage - All workers must make use of the web based services Interviewstreet provides to store all business related materials and content. No files should be stored locally except in situations where off line access is required.

Teleworking

Telecommuting Equipment - Employees working on Interviewstreet business at alternative work sites must use Interviewstreet-provided computer and network equipment, unless other equipment has been approved by the Help Desk as compatible with Interviewstreet information systems and controls.

Telecommuter Working Environments - To retain the privilege of doing off-site work, all telecommuters must structure their remote working environment so that it is in compliance with all Interviewstreet policies and standards.

Telecommuter Information Security Procedures - Telecommuters must follow all remote system security policies and procedures including, but not limited to, compliance with software license agreements and use of shredders to dispose of sensitive paper-resident information.

Remote Workers Required to Sign Specific Policy - All Interviewstreet employees who are approved to work from remote locations must sign an agreement to abide byspecific remote worker policies. The agreement should be reviewedannually.

Organization Property At Alternative Work Sites - The security of Interviewstreet property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable precautions must be taken to protect Interviewstreet hardware, software, and information from theft, damage, andmisuse.

6.0 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.
Interviewstreet does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge ofthe employee's or partner's duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees orpartners that result from violation of thispolicy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or legal@interviewstreet.com as soon aspossible.

7.0 DEFINITIONS

Confidential Information (Sensitive Information) – Any Interviewstreet information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Interviewstreet from a third party under a non-disclosure agreement.

Electronic Messaging System – Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and textmessaging.

Information Asset – Any Interviewstreet data in any form, and the equipment used to manage, process, or store Interviewstreet data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partnerdata.

Objectionable Information or Material – Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by national or international, federal, regional, provincial, state, or local laws.

Partner – Any non-employee of Interviewstreet who is contractually bound to provide some form of service to Interviewstreet.

User - Any Interviewstreet employee or partner who has been authorized to access any Interviewstreet electronic information resource.

8.0 REFERENCES

ISO/IEC 27002 - 7.1.3 Acceptable Use of Assets

9.0 RELATED DOCUMENTS

10.0 APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/2013	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	

Information Security Policies

Amazon Machine Image Policy

Policy #	IS-06	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari Karunanidhi	Phone	

Table of Contents

11.0 Overview

Interviewstreet maintains an environment on Amazon Web Services (AWS). This environment supports the company's day-to-operations and the services that are provided to Interviewstreet customers. The virtual machines that are hosted on AWS are created using Amazon Machine Images (AMI). This policy outlines the creation, use and management of the AMIs that are used as templates for new virtual machines.

12.0 Purpose

This policy defines the requirements for properly and securely using Amazon Machine Images to create new virtual machines within the company's AWS environment.

13.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Interviewstreet, including all personnel affiliated with third parties. This policy applies to all virtual machines that are operated by Interviewstreet.

14.0 Policy

Administrative Access

Training Required – Only Interviewstreet workers that have been trained on the company's policies should be provisioned with administrative access to the hosting environment. This training should include an overview of the current architecture and education on the various AWS services leveraged (eg S3).

Provisioning Required – Access to the AWS administration console requires a workerto first be provisioned within the AWS IAM tool. When a worker is provisioned, they should be placed into the appropriate group, which restricts their access to various AWS services.

AMI Management

Image Creation – Before creating a new AMI that will support a production service, workers need to confirm that none of the AMIs maintained by Interviewstreet will support their business requirements. If a suitable AMI in the company's library cannot be found,workers with the appropriate access to create new AMIs may browse through the AMI Marketplace to find a new AMI. Only AMI's created and supported by Amazon Web Services and the Ubuntu Foundation may be used. At no time should any "community supported" AMIsbe used to create new Interviewstreet images or virtualmachines.

Image Use – Those workers with access to create new virtual machines may use any of the AMI's stored in the company's library. Workers should only use their unique IAM credentials during this process.

Image Maintenance – AMI's that are kept for long-term use within the company'slibrary must be maintained. Maintenance may include the installation of new or updated packages, server configuration changes, etc. All changes made to the AMI's that are kept forlong-term use must be approved by a manager and documented in the AMI's change log on GitHub.

AMI Deployment

Provisioning – Each new virtual machine will need to be assigned to a security group.At no point should a new virtual machine be placed in the company's DMZ or given an elastic IP address without the authorization of the Chief TechnologyOfficer.

Auto Scaling –AMI's that are assigned to an auto scaling group must first approved bythe Chief Technology Officer. Furthermore, no changes should ever be made to an active virtual machine that was created by an auto scaling group. Changes should only be made tothe AMI used by the auto scaling group which will be used to generate new virtual machines that will replace the outdate version.

15.0 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.
Interviewstreet does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge ofthe employee's or partner's duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees orpartners that result from violation of thispolicy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or legal@interviewstreet.com as soon aspossible.

16.0 EXCEPTIONS

Exceptions to this policy must be made in writing by the designated Owner and approved by the CTO.

17.0 DEFINITIONS

Amazon Machine Image – An Amazon Machine Image, or AMI, is an image of a virtual server that can be used as a template to create new servers.

Auto Scaling Group – Auto Scaling Groups are collections of servers that are automatically provisioned and terminated to meet the current customer demand.

Amazon IAM – IAM is the user management interface that is provided by AWS to its customers. It is used to manage worker and machine accounts within the AWS environment.

18.0 REFERENCES

N/A

19.0 RELATED DOCUMENTS

Interviewstreet Acceptable Use Policy,
Interviewstreet Security Group Policy

20.0 APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/2013	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	

Information Security Policies

AWS Remote Access Management Policy

Policy #	IS-04	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari Karunanidhi	Phone	

21.0 Table of Contents

PURPOSE

This policy defines the requirements for establishing the framework and ongoing management of the Interviewstreet AWS remote access infrastructure.

SCOPE

This policy applies to all aspects of Interviewstreet's AWS environment including servers, virtual machines and all services. The target audience of this policy is all Interviewstreet employees who have been provisioned with remote access management responsibilities or who have been given remote access to any Interviewstreet AWS resource.

POLICY

22.0 Program Requirements

Remote Access Strategy Development - Prior to permitting or implementing any remote access to Interviewstreet's AWS environment and systems a detailed analysis must be performed that includes an examination of the risks associated with each solution.

Remote Access Strategy Testing - Before implementing a remote access solution a prototype of the design must be tested and evaluated for security and performance compatibility.

23.0 Documentation and Process

User Management and Provisioning – Users that require access to AWS resources must be provisioned using the company's IAM portal. The provision process must be documented.

Remote Access Processes - Operational processes, such as following the Employee Termination Checklist, must be regularly performed to maintain the security of the remote access infrastructure.

Remote Access Assessments - Audits or assessments must be performed atleast annually to ensure that the Interviewstreet remote access policies, processes, and procedures are being followed.

24.0 Server Configuration

Remote Access Server Isolation - Interviewstreet remote access servers must not be run on the same host as other services and applications.

Remote Access Server Placement - Remote access servers must be placed atthe network perimeter.

Remote Access Server Traffic - VPC security groups must be configured to only allow remote access traffic to originate from the remote access server.

25.0 Authentication and Access

Two-Factor User Authentication - All in-bound access through a public network to every Interviewstreet AWS service or virtual machine must employ two-factor user authentication.

Remote Access Passwords - User IDs with blank or null passwords (passwords with no characters) must not be permitted to gain remote access to any Interviewstreet computer or network.

Privilege Restriction - Need To Know - The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know.

26.0 Data Integrity

Secret Data Transmission - All Interviewstreet secret data transmitted over any communication network must be encrypted.

Standard Encryption Algorithm And Implementation - Encryption must be used to secure remote access traffic using government-approved standard algorithms and standard implementations must be consistently employed.

27.0 Server and Device Management

Remote Access Server and Device Security - All Interviewstreet remote access servers and devices must be kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators.

Remote Access Client Device Support - Support personnel must be properly trained to support remote access users and the software that is used.

28.0 Client Software

Remote Access Client Software Configuration - Remote access client software must be configured to provide Interviewstreet with nearly complete control over the remote access environment.

29.0 Device Management and Security

Remote Access Device Management Training - All Interviewstreet employees who are responsible for the management of any AWS virtual machines or services must be trained to properly secure these devices.

Remote Access Server and Device Security - All Interviewstreet remote access servers and devices must be kept fully patched, operated using Interviewstreet's baseline AMI, and only managed from trusted hosts by authorized administrators.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Interviewstreet does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

DEFINITIONS

Confidential Information (Sensitive Information) - Any Interviewstreet information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts.

Confidential Information also includes any confidential information received by Interviewstreet from a third party under a non-disclosure agreement.

Remote Access Device - Any electronic mechanism that is used to connect and transmit information to and from a remote access server, e.g., personal and portable computers, personal digital assistants, smart phones, etc.

Remote Access Server - The computer and associated software that is set up to handle users seeking access to a network from a location that is not directly connected to that network. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

Two-Factor Authentication - A security process in which the user provides two means of identification, one of which is typically a physical token, such as a card or one-time password generator, and the other of which is typically something memorized, such as a security code that is directly associated with the token. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A common example of two-factor authentication is a bank card: the card, something you have, and the personal identification number (PIN), something you know.

REFERENCES

ISO/IEC 27002 - 11.7.1 Mobile Computing and Communications

RELATED DOCUMENTS

Interviewstreet Acceptable Use Policy

APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/3012	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	

Information Security Policies

Backup and Restore Policy

Policy #	IS-02	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari Karunanidhi	Phone	

Table of Contents

30.0 PURPOSE

This policy defines the requirements for maintaining and restoring backup copies of sensitive Interviewstreet customer information created, processed, or stored on Interviewstreetvirtual machines and databases.

31.0 SCOPE

This policy applies to all customer data with a target audience of Administrator and Developers.

32.0 POLICY

Schedule

Data Backups - All Customer Data stored on Interviewstreet databases must be periodically backed-up on a daily basis.

Backup Process - Database snapshots must be scheduled to run automatically every 24 hours.

Critical Information Backups - All Customer Data must be backed-up at least quarterly onto a different storage media, such as Amazon Glacier, and kept for at least one year.

Procedures

On-Site Backup Files - At least one generation of backup files must be maintained onoff- line data storage media wherever production computers are located.

Multiple Backup Copies - At least two recent and complete backups made ondifferent dates containing critical Interviewstreet records must always be stored off-site.

Critical Backup Files - Critical data that has been backed up must not be used for data restoration purposes unless another backup copy of the same data exists ondifferent computer storage media. If this additional copy does not presently exist, before the restoration, the copy must first be made on a computer other than the one where the restoration is to take place.

All Electronic Communications Are Recorded And Archived - All electronic communications sent through Interviewstreet networks, including electronic mail and instant messages are both recorded and archived.

Copies Of Sensitive, Critical, Or Valuable Information - Unless other backup arrangements are known to be operational, all end users are responsible for making at least two current backup copies of critical files each time that a significant number of changes are saved.

Information Preservation After Application Decommission - Before anyInterviewstreet product applications are taken out of production, a final backup of all sensitiveproduction data must be made and preserved for at least three (3) years. Backup media that store this production data must contain a classification label which matches the highest (most sensitive) classification of the data being stored.

Media

Backup Media Storage - Essential business information and software backups must be stored in an environmentally protected and access-controlled site that is a sufficientdistance away from the originating facility.

Archival Storage Directory - All archival backup data stored off-site must be reflected in a current directory that shows the date when the information was most recently modified and the nature of the information.

Archival Storage Preservation - Computer media storage procedures must assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to deterioration.

Backup Media Encryption - All sensitive, valuable, or critical information recorded on backup computer media and stored outside Interviewstreet offices must beencrypted.

Testing and Review

Archival Storage Media Testing - Critical business information and critical software archived on storage media, such as S3 or Glacier, for a prolonged period of time must be tested at least annually to provide assurance that they can be fully recovered.

Archival Storage Media Quality - The computer data media used for storingsensitive, critical, or valuable information must be high quality and must be periodically testedfor reliability.

Backup Review - Managers or their delegates must ensure that proper backups of sensitive, critical and valuable data are being made if such data is resident onpersonal computers, workstations, or other small systems in their area.

33.0 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Interviewstreet does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

34.0 DEFINITIONS

Backup - A copy of files and programs made to facilitate recovery if necessary.

Confidential Information (Sensitive Information) – Any Interviewstreet information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Interviewstreet from a third party under a non-disclosure agreement.

Information Asset - Any Interviewstreet data in any form, and the equipment used to manage, process, or store Interviewstreet data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Partner - Any non-employee of Interviewstreet who is contractually bound to provide some form of service to Interviewstreet.

35.0 REFERENCES

ISO/IEC 27002 - 10.5.1 Information back-up

36.0 RELATED DOCUMENTS

Interviewstreet Acceptable Use Policy

37.0 APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/2013	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	

Information Security Policies

Incident Reporting and Response Policy

Policy #	IS-07	Effective Date	09/10/2014	Email	support@hackerrank.com
Version	1.0	Contact	HR Support	Phone	415.900.4023

Table of Contents

PURPOSE

This policy defines the requirements for reporting and responding to incidents related to HackerRank information systems and operations.

SCOPE

This policy applies to all employees, consultants, contractors, or agents of HackerRank and any of its entities including, but not limited to, business units and subsidiaries, and to any computing devices owned or leased by HackerRank and any of its entities.

POLICY

Roles and Responsibilities

Incident Response Team - The HackerRank Incident Response Team, as organized by HackerRank's management, shall be responsible for monitoring and responding to alerts that include but are not limited to evidence of unauthorized activity, detection of unauthorized access, critical IDS alerts, and reports of unauthorized critical system or content file changes.

Incident Response Team Availability - The HackerRank Incident Response Team must be available at all times to respond to such alerts.

Display of Incident Reporting Contact Information - HackerRank contact information and procedures for reporting information security incidents must be prominently displayed and easily accessible. The Incident Response Team must periodically test the communications system(s) permitting notification of suspected information security problems.

Identification

Incident - The term "incident" refers to an adverse event impacting one or more HackerRank's information assets or to the threat of such an event. Examples include but are not limited to the following:

- Unauthorized use
- Denial of Service
- Malicious Code
- Malware
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information Security Breach

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of employees
- Actions of vendors or contractors
- Actions of third parties
- External or internal acts
- Potential violations of HackerRank policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing

Procedures

Incident Handling - The following is a list of response priorities that should be reviewed and followed as recommended by the Incident Response Team:

- **Safety and Human Issues** - If an information system involved in an incident affects human life and safety, responding to any incident involving any life-critical or safety-related system is the most important priority.
- **Address Urgent Concerns** - Urgent concerns about the availability or integrity of critical systems or data must be addressed promptly.
- **Establish Scope of Incident** - The Incident Response Team shall promptly work to establish the scope of the incident and to identify the extent of systems and data affected. If it appears that personally identifiable information may have been compromised, the Incident Response Team shall immediately inform HackerRank's management and legal teams.
- **Containment** - Once life-critical and safety issues have been resolved, the Incident Response Team shall identify and implement actions to be taken to reduce the potential for the spread of an incident or its consequences across additional systems and networks.
- **Develop Plan for Preservation of Evidence** - The Incident Response Team shall develop a plan promptly upon learning about an incident for identifying and implementing appropriate steps to preserve evidence, consistent with needs to restore availability. Preservation plans may include preserving relevant logs and screen captures. The affected system may not be rebuilt until the Incident Response

Team determines that appropriate evidence has been preserved. Preservation will be addressed as quickly as possible to restore availability that is critical to maintain business operations.

- **Investigate the Incident** - The Incident Response Team shall investigate the causes of the incident and future preventative actions. During the investigation phase, members of the Incident Response Team will attempt to determine exactly what happened during the incident, especially the vulnerability that made the incident possible.
- **Incident-Specific Risk Mitigation** - The Incident Response Team shall identify and recommend strategies to mitigate risk of harm arising from the incident, including but not limited to reducing, segregating, or better protecting personal, proprietary, or mission critical data.
- **Threat/Vulnerability Eradication** - After an incident is mitigated, the Incident Response Team's efforts will focus on identifying, removing and repairing any vulnerability that led to the incident and thoroughly cleaning the system. To do this, the vulnerability(s) needs to be clearly identified. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been resolved.
- **Confirmation** - After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced.
- **Restore Availability** - Once the above steps have been taken, and upon authorization by the Incident Response Team, the availability of affected devices or networks may be restored and normal operations may resume.
- **Reporting** - The Incident Response Team shall develop and arrange for implementation of a communications plan to spread learning from the incident throughout HackerRank to individuals best able to reduce risk of recurrence of such incident.

Incident Analysis and Reporting - An after-action analysis will be performed for all incidents. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meetings should be held by the Incident Response Team within one week of closing the incident.

- **Notification –** If sensitive and/or personally identifiable information is compromised as a result of the incident, HackerRank shall notify individuals whose information may have been at risk as required by law.

- **Communication –** The Incident Response Team will review and approve any communication regarding the incident for accuracy and clarity.

Documentation - The Incident Response Team shall:

- **Log of security incidents** - The Incident Response Team will maintain a log of all incidents recording the date, systems affected, the type of data affected (if any), number of subjects (if applicable), and a summary of the reason for the incident, and the corrective measure(s) taken.
- **Critical Incident Report** - The Incident Response Team will issue a Critical Incident Report for every incident affecting critical hosts or other priority incidents. Each Critical Incident Report will describe in detail the circumstances that led to the incident, and a plan to eliminate the risk.

Security Changes After System Compromise - Whenever a system has been compromised, or suspected of being compromised by an unauthorized party, all recent changes to user and system privileges must be reviewed for unauthorized modifications.

Suspected System Intrusions - Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and analyzed to ensure that the system is free of compromise before reconnecting it to the network.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. HackerRank reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Malicious Code - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

Malware - A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

REFERENCES

ISO/IEC 27002 – 13.0 Information Security Incident Management

Approval and Ownership

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	09/10/2014	
Approved By	**Title**	**Date**	**Signature**
Marie Noto	Legal Counsel	09/10/2014	

Information Security Policies

Information Classification Policy

Policy #	IS-01	Effective Date	12/11/2014	Email	hari@HackerRank.com
Version	1.0	Contact	Hari K	Phone	

Table of Contents

38.0 Purpose

This policy is designed to support the “need to know” principle so that information may be protected from unauthorized disclosure, use, modification, and deletion. Consistent use of this data classification system will facilitate business activities.

39.0 Scope

This Information Classification policy applies to all information in possession of HackerRank. No distinctions between the word “data”, “information”, “knowledge,” and “wisdom” are made for purposes of this policy.

40.0 Policy

Public (Class 1)

This classification applies to information that is available to the general public and intended for distribution outside the organizations. This information may be freely disseminated without potential harm. It is also defined as Non-sensitive information available for external release. Examples include: name of the test, instructions to take the test, any other information that can be found on the test landing page of HackerRank.

Internal (Class 2)

For internal use only. This classification applies to all other information that does not clearly fit into the other classifications. The unauthorized disclosure, modification or destruction of this information is not expected to seriously or adversely impact the organization, its employees, or its business partners. Examples include the company telephone directory, new employee training materials, and internal policy manuals. Information that is generally available to employees and approved non-employees.

Confidential (Class 3)

Information that is sensitive within the company and is intended for use only by specified groups of employees. In other words, this classification applies to information that is intended for use within the organization. Its unauthorized disclosure could adversely impact the organization, its employees and its business partners. Information that some people would consider private is included in this classification. Examples include email address of recruiters and candidates.

Highly Critical (Class 4)

Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a highly critical manner. In other words, this can be defined as information that is considered highly critical by the company. The examples for this include questions for the tests.

41.0 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. HackerRank reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. HackerRank does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, HackerRank reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or legal@HackerRank.com as soon as possible.

42.0 DEFINITIONS

Confidential Information (Sensitive Information) – Any HackerRank information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by HackerRank from a third party under a non-disclosure agreement.

Information Asset – Any HackerRank data in any form, and the equipment used to manage, process, or store HackerRank data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Partner – Any non-employee of HackerRank who is contractually bound to provide some form of service to HackerRank.

User - Any HackerRank employee or partner who has been authorized to accessany HackerRank electronic information resource.

43.0 REFERENCES

http://www.datasecuritypolicies.com/sample-data-classification-policy/

44.0 RELATED DOCUMENTS

N/A

45.0 APPROVAL ANDOWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	12/11/2014	
Approved By	**Title**	**Date**	**Signature**
Darshan Suresh	Solutions Engineer	12/11/2014	

Information Security Policies

Password Management Policy

Policy #	IS-03	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari Karunanidhi	Phone	

46.0 Table of Contents

PURPOSE

This policy defines the requirements for establishing the password configuration settings and managing fixed passwords used on any Interviewstreet computer and communications system.

SCOPE

This policy applies to all information developers and system administrators responsible for the maintenance of password management systems and user accounts on Interviewstreet electronic information resources.

POLICY

47.0 Distribution

Initial Passwords - Passwords issued by an administrator must be expired, forcing the user to choose another password before the next logon process is completed.

Password Sharing - Passwords must never be shared or revealed to anyone other than the authorized user.

In-Person Password Authentication - A user must be authenticated in person to obtain a new or changed password.

Initial Password Transmission - The initial password for a new remote user must be sent through a communications channel other than the channel used to log on to Interviewstreet systems including, but not limited to, courier service requiring a signature, and in-person appearance at a trusted intermediary's office along with the provision of picture identification.

Sending Passwords By Mail - If sent by regular mail or similar physical distribution systems, passwords must be sent separately from user IDs, have no markings indicating the nature of the enclosure and be concealed inside a sealed opaque envelope that will readily reveal tampering.

Disclosure Of Passwords - Security Administrators must disclose passwords to a user providing two pieces of definitive evidence substantiating his or her identity only if a new user ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of his or her user ID.

48.0 Resets

Password Resets – Identification - The requesting user must be positively identified before a password reset may be performed.

Password Resets - Unique Value - Password issued as a result of a requested reset must be a unique value, i.e. a string of characters that is not the same for all password resets.

Fixed Password Change Confirmation - All fixed password resets or changes must be promptly confirmed by regular mail so that the authorized user can readily detect and report any fraudulent or abusive behavior. The password itself must not be transmitted -- only the fact that it was changed.

49.0 Compromised Passwords

Password Changes After System Compromise - If a multi-user computer system employs fixed passwords as its primary access control mechanism, all passwords on that system must be changed immediately after evidence of system compromise has been discovered, and all users must change their fixed passwords on other machines, if the passwords on the compromised machine are also used on these other machines.

Password Changes After Privileged User ID Compromise - If a privileged user ID has been compromised by an intruder or another type of unauthorized user, all passwords on that system must be immediately changed.

Passwords Set To Expired After Intrusion - After either a suspected or demonstrated intrusion to a Interviewstreet computer system, the involved System Administrator must immediately notify the system's user community that an intrusion is believed to have taken place. The status of all passwords on that system must immediately be changed to expired, so that these passwords will be changed at the time that the involved users next log-in.

50.0 Composition

Password Characters - All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character.

Password Case - All user-chosen passwords must contain at least one lower case andone upper case alphabetic character.

Null Passwords Always Prohibited - At no time, may any Systems Administratoror Developer enable any user ID that permits password length to be zero (a null or blank password).

51.0 Length

Minimum Password Length - All passwords must have at least 8 characters and this length must always be checked automatically at the time that users construct or selecttheir password.

Minimum Password Length Constraint - User-chosen fixed passwords must be at least8 characters long, or the maximum length permitted by the system if this is less than 8 characters.

Role-Based Password Length - The minimum length for fixed passwords must be set to four for voice mail boxes and handheld computers and ten for administrator and other privileged user IDs.

52.0 Generation

System-Generated Passwords - All system-generated passwords for end users mustbe pronounceable.

System-Generated Password Issuance And Storage - If passwords or personal identification numbers are generated by a computer system, they must always beissued immediately after they are generated and must never be stored on the involvedcomputer systems.

Seed For System-Generated Passwords - If system-generated passwords are used,they must be generated using the low order bits of system clock time or some other very- frequently-changing and unpredictable source.

53.0 History

Password History - On all multi-user Interviewstreet computers, system software or locally-developed software must be used to maintain an encrypted history of previouslychosen fixed passwords. This history must contain at least the previous thirteen passwords for each user ID.

54.0 Changes

Required Password Changes - All users must be automatically required to change their passwords at least once every 90 days.

Masking Password Changes - Whenever user-chosen passwords or encryption keys are specified, they must be entered twice and masked such that the user cannot see whatwas typed.

Password Change Interval Synchronization - The fixed password change interval must be synchronized across all computer and network platforms atInterviewstreet.

User Notification Of Changed Password - Whenever a fixed password is changed, the involved user must be promptly notified of that fact using a communications systemother than the one to which the password applies. This notification must be accompanied by instructions to immediately contact the Support team if the authorized user did notinitiate the change.

Customers Account Password Reset Attempts - Interviewstreet must limit the number of attempts by online account customers to reset their passwords or login credentials to a maximum of three attempts. After the maximum attempts, the accounts will betemporarily disabled.

Password Reset After Lockout - All Interviewstreet computer systems that employfixed passwords at log on must be configured to permit only three attempts to enter acorrect password, after which the user ID is deactivated and can only be reset by the HelpDesk staff after authenticating the user's identity. This applies to all user accounts that are managed by AWS IAM and Google Apps.

55.0 Display

Password Display And Printing - The display and printing of passwords, when end users enter them, must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recoverthem.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.
Interviewstreet does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge ofthe employee's or partner's duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees orpartners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon aspossible.

DEFINITIONS

Partner – Any non-employee of Interviewstreet who is contractually bound to provide some form of service to Interviewstreet.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

System Administrator – An employee or partner who is responsible for managing a Interviewstreet multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

User - Any Interviewstreet employee or partner who has been authorized to access any Interviewstreet electronic information resource.

REFERENCES

ISO/IEC 27002 - 11.2.3 User Password Management

RELATED DOCUMENTS

Interviewstreet Acceptable Use Policy

APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/2013	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	

Information Security Policies

Password Management Policy

Policy #	IS-03	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari Karunanidhi	Phone	

56.0 Table of Contents

PURPOSE

This policy defines the requirements for establishing the password configuration settings and managing fixed passwords used on any Interviewstreet computer and communications system.

SCOPE

This policy applies to all information developers and system administrators responsible for the maintenance of password management systems and user accounts on Interviewstreet electronic information resources.

POLICY

57.0 Distribution

Initial Passwords - Passwords issued by an administrator must be expired, forcing the user to choose another password before the next logon process is completed.

Password Sharing - Passwords must never be shared or revealed to anyone other than the authorized user.

In-Person Password Authentication - A user must be authenticated in person to obtain a new or changed password.

Initial Password Transmission - The initial password for a new remote user must be sent through a communications channel other than the channel used to log on to Interviewstreet systems including, but not limited to, courier service requiring a signature, and in-person appearance at a trusted intermediary's office along with the provision of picture identification.

Sending Passwords By Mail - If sent by regular mail or similar physical distribution systems, passwords must be sent separately from user IDs, have no markings indicating the nature of the enclosure and be concealed inside a sealed opaque envelope that will readily reveal tampering.

Disclosure Of Passwords - Security Administrators must disclose passwords to a user providing two pieces of definitive evidence substantiating his or her identity only if a new user ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of his or her user ID.

58.0 Resets

Password Resets – Identification - The requesting user must be positively identified before a password reset may be performed.

Password Resets - Unique Value - Password issued as a result of a requested reset must be a unique value, i.e. a string of characters that is not the same for all password resets.

Fixed Password Change Confirmation - All fixed password resets or changes must be promptly confirmed by regular mail so that the authorized user can readily detect and report any fraudulent or abusive behavior. The password itself must not be transmitted -- only the fact that it was changed.

59.0 Compromised Passwords

Password Changes After System Compromise - If a multi-user computer system employs fixed passwords as its primary access control mechanism, all passwords on that system must be changed immediately after evidence of system compromise has been discovered, and all users must change their fixed passwords on other machines, if the passwords on the compromised machine are also used on these other machines.

Password Changes After Privileged User ID Compromise - If a privileged user ID has been compromised by an intruder or another type of unauthorized user, all passwords on that system must be immediately changed.

Passwords Set To Expired After Intrusion - After either a suspected or demonstrated intrusion to a Interviewstreet computer system, the involved System Administrator must immediately notify the system's user community that an intrusion is believed to have taken place. The status of all passwords on that system must immediately be changed to expired, so that these passwords will be changed at the time that the involved users next log-in.

60.0 Composition

Password Characters - All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character.

Password Case - All user-chosen passwords must contain at least one lower case and one upper case alphabetic character.

Null Passwords Always Prohibited - At no time, may any Systems Administrator or Developer enable any user ID that permits password length to be zero (a null or blank password).

61.0 Length

Minimum Password Length - All passwords must have at least 8 characters and this length must always be checked automatically at the time that users construct or select their password.

Minimum Password Length Constraint - User-chosen fixed passwords must be at least 8 characters long, or the maximum length permitted by the system if this is less than 8 characters.

Role-Based Password Length - The minimum length for fixed passwords must be set to four for voice mail boxes and handheld computers and ten for administrator and other privileged user IDs.

62.0 Generation

System-Generated Passwords - All system-generated passwords for end users must be pronounceable.

System-Generated Password Issuance And Storage - If passwords or personal identification numbers are generated by a computer system, they must always be issued immediately after they are generated and must never be stored on the involved computer systems.

Seed For System-Generated Passwords - If system-generated passwords are used, they must be generated using the low order bits of system clock time or some other very- frequently-changing and unpredictable source.

63.0 History

Password History - On all multi-user Interviewstreet computers, system software or locally-developed software must be used to maintain an encrypted history of previously chosen fixed passwords. This history must contain at least the previous thirteen passwords for each user ID.

64.0 Changes

Required Password Changes - All users must be automatically required to change their passwords at least once every 90 days.

Masking Password Changes - Whenever user-chosen passwords or encryption keys are specified, they must be entered twice and masked such that the user cannot see what was typed.

Password Change Interval Synchronization - The fixed password change interval must be synchronized across all computer and network platforms at Interviewstreet.

User Notification Of Changed Password - Whenever a fixed password is changed, the involved user must be promptly notified of that fact using a communications system other than the one to which the password applies. This notification must be accompanied by instructions to immediately contact the Support team if the authorized user did notinitiate the change.

Customers Account Password Reset Attempts - Interviewstreet must limit the number of attempts by online account customers to reset their passwords or login credentials to a maximum of three attempts. After the maximum attempts, the accounts will betemporarily disabled.

Password Reset After Lockout - All Interviewstreet computer systems that employfixed passwords at log on must be configured to permit only three attempts to enter acorrect password, after which the user ID is deactivated and can only be reset by the HelpDesk staff after authenticating the user's identity. This applies to all user accounts that are managed by AWS IAM and Google Apps.

65.0 Display

Password Display And Printing - The display and printing of passwords, when end users enter them, must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recoverthem.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.
Interviewstreet does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge ofthe employee's or partner's duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees orpartners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon aspossible.

DEFINITIONS

Partner – Any non-employee of Interviewstreet who is contractually bound to provide some form of service to Interviewstreet.

Password – An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

System Administrator – An employee or partner who is responsible for managing a Interviewstreet multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks.

User - Any Interviewstreet employee or partner who has been authorized to access any Interviewstreet electronic information resource.

REFERENCES

ISO/IEC 27002 - 11.2.3 User Password Management

RELATED DOCUMENTS

Interviewstreet Acceptable Use Policy

APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/2013	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	

Information Security Policies

Security Group Management Policy

Policy #	IS-05	Effective Date	07/01/2013	Email	hari@interviewstreet.com
Version	1.0	Contact	Hari Karunanidhi	Phone	

Table of Contents

66.0 Purpose

This policy defines the essential rules regarding the management and maintenance of security groups at Interviewstreet and it applies to all security groups managed by Interviewstreet workers.

67.0 Scope

This policy applies to all Interviewstreet security groups. This policy applies to all security groups managed by employees. Exception will be permitted only if approved in advance and in writing by the Information CTO.

68.0 Policy

Business Justification

Standard Security Groups - The security groups appearing on the attached list of approved security groups are the only ones that may be deployed in Interviewstreet's virtual computing environment.

Machine Specific Security groups - All virtual machines needing greater protection than what can be provided by the standard security group(s) closer to the edge of the network -- as determined by due care or by a risk assessment -- will require implementation of a non machine security group. As with all other Interviewstreet security groups, the machine specific security group is to be based on the Interviewstreet's template.

Security Group Dedicated Functionality – Interviewstreet security groups are role specific and should be associated with a specific business need (eg Web Server, Code Checker, etc). To the extent the supporting VPC allows it, all unnecessary and unused services and ports must be restricted in Company security groups.

Required Documentation - Prior to the deployment of every Interviewstreet security group, a diagram and/or list of permissible paths and a description of permissible services accompanied by a justification for each, must be submitted to theCTO.

Access Approval - Permission to enable such paths and services is granted by the CTO only when these paths or services are necessary for important business reasons, and sufficient security measures will be consistently employed. Any changes to paths orservices must go through this same process as follows.

Implementation

Connections Between Machines - Real-time connections between two or more Interviewstreet computer systems are not be established or enabled unless it has been determined that such connections will not unduly jeopardize information security. Inmany cases, security groups or similar intermediate services must be employed. Any connection between an Interviewstreet production system and any external system, or any external computer network or service provider, must be approved in advance by theCTO.

External Connections - All in-bound real-time Internet connections to Interviewstreet's VPC must pass through a security group before users can reach a logon banner. Interviewstreet virtual machines may be given an Elastic IP address, or a publically routable IP address, to the Internet only when protected by a security group. Wherever a virtual machine supports it, logon screens display a notice indicating that the system may be accessed only by authorized users, users who log on represent that they are authorized to do so, unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and system usage will be monitored andlogged.
Virtual Private Networks - All inbound traffic to the VPC, with the exception of Internet mail, must be encrypted with the one of the approved VPNmethodologies.

Secured Subnets - Portions of the Interviewstreet internal network that contain sensitiveor valuable information must employ a secured subnet. In the Interviewstreet VPC, each secure subnet has a security group that meets the business requirements of those virtual machines. Access to this and other subnets must be restricted with security groups and other access control measures. Based on periodic risk assessments, the CTO will define the secured subnets required in the Information SecurityArchitecture.

Demilitarized Zones - All web servers must be protected by security groups, and be located within a demilitarized zone (DMZ), and placed within a subnet with other machines with similar access. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more security groups.

Disclosure Of Internal Network Information - The internal system addresses, configurations, products deployed, and related system design information for networked computer systems are restricted to preclude both systems and users outside the Interviewstreet internal network from accessing this information. Network Address Translation (NAT) is the preferred method for protecting internal IP addresses. Configuration and operation standards are implemented and maintained to preclude internal business information from being resident on or processed by any security group, server, or other computer that is shared with another organization at an outsourcingfacility.
Default To Denial - Every connectivity path and service not specifically permitted by this standard and supporting documents issued by the Information Security department is blocked by default by Interviewstreet's securitygroups.

Authentication Administrative Users - Inbound traffic -- with the exception of Internet electronic mail, regular news distributions, and push broadcasts previously approved by the CTO -- require the following extended user authentication measures documented below.

- Digital Certificates: Each administrator will generate a unique public/private SSH key which will then be installed on the VPC's VPN. This key can be revoked if/when the user has a change in permissions or employment.
- IAM Provisioning: Each administrator will be provisioned using IAM. They will receive a unique user name and password in addition to an API key for their daily work.

Security group Access Mechanisms - All security groups are to be configured through the AWS web based interface or API. Group User IDs are not allowed and the same password or access control code must not be used. Security group administrators are required to use extended user authentication mechanisms to access any of the Interviewstreet's security groups.

Security group Access Privileges - Privileges to modify the functionality, connectivity, and services supported by security groups is restricted to the Security group in IAM. Unless the CTO has granted permission otherwise, Security group workers are limited to individuals who are permanent Company employees, and not temporaries, contractors, consultants, or outsourcing personnel. All security groups must have at least two staff members who are adequately trained to make changes as circumstances require. Such training includes periodic refresher training course or conference attendance to permit these staff members to stay current with the latest developments in security group technology and security group operations. Staffing and scheduling must ensure that at least one of these security group administration staff members is readily available at all times.

Security group Operation

Monitoring Vulnerabilities – Security group Administrators are expected to subscribe to the most appropriate Internet alert advisories available and other relevant sources providing current information about AWS vulnerabilities. Any vulnerability that appears to affect Interviewstreet networks and systems must promptly be brought to the attention of the CTO.

Vulnerability Scans – All security groups must be verified by at least one or more of the vulnerability scanning methods\systems. This includes Nessus and NMap scans.

Discrepancies between the security group's Approved Paths and the results of a scan should be documented in a GitHub issue and assigned to the appropriate employee.

Security group Logs – AWS does not provide access to security groups logs. This is true for all customers who use AWS, inside and outside of a VPC.

Change Management

Production Security Group Change Management – Because security groups are critical systems, major changes to the internal networking environment, any changes to the production business applications supported, and any major information security incident triggers an additional and immediate review of the security group policy. In addition tohe same documentation that is required for changes on production systems, security group changes require the additional process as follows.

Security group Rule (aka "Policy") Change Management Process – All changes to a security group rule-set (aka "policy") require the following process over and above the standard Change Management process:

1. All security group rule change requests must include the following pieces of information:
    a. Source address(es), including IP's and domain names (where applicable)
    b. Destination address(es), including IP's and domain names (where applicable)
    c. Port(s) and Service(s) requested to be open
    d. Date when the change should be made
    e. Point of contact
2. Each request should be logged as an issue in GitHub with the required information and assigned to the CTO
3. All security group rule change requests will be evaluated to ensure that they conform to current security best practices and current Interviewstreet security policy.

Continuity Management

Continuity Planning – Administrators must prepare and maintain continuity plans which specify the actions to be taken in the event of disruptions such as system compromise, malfunction, crash, or overload, and Internet service provider unavailability. Such plans are prepared and maintained per Company specifications. These contingency plans must be kept current to reflect changes in the Company's information systems environment and periodically tested to ensure effective restoration of a secure and reliable networking environment.

Regular Testing - The proper configuration of Company security groups are tested on a regular basis, according to this policy. This testing uses software agents that automatically check to determine whether security groups are configured and running in a manner that is consistent with Interviewstreet security policies and the relevant security group documentation. This testing process includes consideration of defined configuration parameters, enabled services, and permitted connectivity paths. These tests also include periodic execution of vulnerability identification software and the regular performance of penetration tests.

69.0 VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Interviewstreet reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.
Interviewstreet does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Interviewstreet reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager or any other manager as soon as possible.

70.0 DEFINITIONS

Demilitarized Zone (DMZ) - An interface on a routing security group leading to a protected network that is different from the main network protected by the security group. Traffic bound for the DMZ still goes through the security group, and can have the security group's protection policies applied.

Deny by Default - To block all inbound and outbound traffic that has not been expressly permitted by security group policy.
Security Group Policy - A security group policy defines how an organization's security groups should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.

Network Address Translation (NAT) - Used to hide internal system addresses from an external network through use of an addressing schema.

Ruleset - A set of directives that govern the access control functionality of a security group. The security group uses these directives to determine how packets should be routed between its interfaces.

Security Group - A security group acts as a firewall that controls the traffic for one or more instances.
Virtual Private Network (VPN) - VPNs use additional protocols to encrypt and decrypt specific network traffic flows between the protected network and external networks and provide user authentication and integrity checking. VPNs are most often used to provide secure network links across untrusted networks. Two common choices for secure VPNs are Internet Protocol Security (IPsec)3 and Secure Sockets Layer (SSL)/Transport Layer Security (TLS).4

Virtual Private Cloud - Amazon Virtual Private Cloud (Amazon VPC) enables a customer to launch Amazon Web Services (AWS) resources into a virtual network that they have defined. This virtual network closely resembles a traditional network that a customer would operate in their own data center, with the benefits of using the scalable infrastructure of AWS.

71.0 References

ISO 27002 - 7.1.3 Acceptable use of assets AWS Security
Group Documentation
AWS Virtual Private Cloud Documentation

72.0 Related Documents

Attachment A: "Interviewstreet Network Diagram" Interviewstreet AMI
Policy
Interviewstreet Acceptable Use Policy

73.0 Approval and Ownership

Owner	Title	Date	Signature
Hari Karunanidhi	CTO	07/01/2013	
Approved By	**Title**	**Date**	**Signature**
Paul Barber	VP of Sales	07/01/2013	