**BlackRock INC. Password Policy**

**By**

**Natnael kebede**

**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 8396 – Strategic Cybersecurity Practicum

Summer 2020

Presented to Professor Brian Wrozek

# **Table of Contents**

[Overview 3](#_Toc43067835)

[Purpose 3](#_Toc43067836)

[Scope 4](#_Toc43067837)

[Policy 4](#_Toc43067838)

[Password Construction 4](#_Toc43067839)

[Password Protection 5](#_Toc43067840)

[General Password Guidelines 6](#_Toc43067841)

[Policy Enforcement and Violations 7](#_Toc43067842)

[Limitations of Liability 7](#_Toc43067843)

[Policy Review and Modification 7](#_Toc43067844)

[Related Standards and Policies 8](#_Toc43067845)

[Revision History 8](#_Toc43067846)

[Appendix 9](#_Toc43067847)

[Policy Compliance and Auditing 9](#_Toc43067848)

[References 10](#_Toc43067849)

ii

# Overview

Passwords are a critical component of information security. They are the primary means to protect user accounts and data stored on systems from unauthorized exposure, allowing associates to uphold the confidentiality, integrity, and availability of corporate information. As a result, the importance of strong and secure passwords is crucial to preserve and utilize data needed to meet BlackRock Inc.’s business objectives, including providing risk management, advisory, and investment solutions that range from active management methods that maximize performance, to well-optimized indexing plans that provide comprehensive exposure to world capital markets (BlackRock Incorporated, 2019).

To provide these services, BlackRock has several password-protected computer systems (both connected and not connected), including and not limited to computers (such as laptops, tablets, and desktops), and hot-plug devices (such as USB drives and external drives), network, email, and corporate social media accounts.

# Purpose

This policy aims to ensure all BlackRock Inc’s computer systems and data receive adequate password protection. The policy covers best practices for the creation of secure and robust passwords, the protection of such passwords, and the frequency of change.

The information security department, being a critical function to the organization, seeks to support BlackRock in achieving its corporate philosophy and principles with this policy with its commitment to protecting the company's compute and network infrastructure from damaging activities, intended or otherwise by equipment or individuals.

# Scope

The scope of this policy applies to employees, contractors, consultants, and other workers who own an account or are responsible for it. Such accounts guidelines apply to all passwords pertaining but not limited to user-level accounts, system-level accounts, web accounts, email accounts, local network log-in accounts, and corporate social media accounts.

To be effective in achieving the security and protection policies detailed in this document, it will take a collaborative effort that entails the participation, feedback, and the support of all BlackRock employees who make use of the related intellectual property, information and information systems. Therefore, as stipulated in these guidelines, the above personnel and related stakeholders who perform businesses using the above types of accounts are responsible.

# Policy

## Password Construction

All in-scope users and personnel of BlackRock Inc. stated above should be aware of how to create secure and robust passwords as outlined in the guidelines below.

|  |  |  |
| --- | --- | --- |
| **Statement of Guidance** | **Description** | **Sample** |
| Strong password on Systems and Accounts. | The password should contain a minimum of 12 characters with a combination of lower- and upper-case letters, numbers, punctuation, and special characters (e.g., @#$%^?&\*()\_+|~-=\`{}[]:";'<>/.etc.)  Another option for password construction is to use passphrases. That is, a passphrase is not the same as a password. Instead, it is a longer version of a password, and hence more secure. We recommend a long sentence passphrase (more than 12 characters) that is easy to remember and contains a combination of lower- and upper-case letters, numbers, punctuation, and special characters (e.g., @#$%?^&\*()\_+|~-=\`{}[]:";'<>/. etc.)  **Note:** The rules that apply to passwords apply to passphrases too. | Amaz!ng@123#Welcome.  BatmanVs.Superman,wh0wi11win?  **Note:** These are meant to be samples. Do not use any of them directly! Instead, create your own unique password or passphrase. |

On the other hand, the construction of weak passwords with the following characteristics are entirely unacceptable and should always be avoided.

1. Limited Passwords: During the registration of a new account or password reset, BlackRock’s portals will inhibit the acceptance of passwords that do not meet the above stated strong password on systems and accounts guidelines. The portals will display the requirements for password construction for every failed attempt to create a secure and robust password.
2. Common Characteristics in Passwords: Avoid using names such as BlackRock, your own name, friend’s/colleagues’ name when creating a password. Additionally, avoid personal information such as SSN, phone number, address, and repeated patterns such as ‘abcdabacd’, “12341234”, or common password such us “Mypassword123.” Instead, create passwords that are unique to you and easy to remember (“Password Construction Guidelines”, 2017).

## Password Protection

As an account owner at BlackRock Inc., you are strictly required to follow the following measures to avoid any credentials from being compromised.

* Create and utilize different passwords to access resources such as applications, systems, and virtual private networks (VPNs). To enable employees to maintain multiple passwords, we highly suggest using the Dashlane password manager application installed on devices.
* Avoid sharing your credentials and password with others by any means, including but not limited to email, chat, or paper. If someone keeps demanding for your password, instruct them to contact the information security department via email: [infosec@blackrock.](mailto:infosec@blackrock.net)com

Additionally, refrain from preserving your password on paper or your desk.

* Avoid using the “Remember Password” option in browsers (“Password Protection Guidelines”, 2017). If you do not remember your password the next time you log-in, use the password reset option. Note that personalized security questions must be set up to use this technique to reset your passwords. Contact the solution center via email: [helpdesk@blackrock.](mailto:helpdesk@blackrock.net)com if you encounter problems in doing so.
* Refrain from talking about or hinting other about your password. Furthermore, enable multi-factor authentication through DUO or Microsoft Authenticator application depending on the type of resource you are accessing.
* In the instance that you believe your credential is compromised, change all passwords and report the incident to [incidents@blackrock.](mailto:incidents@blackrock.net)com with the subject line “Password Compromise”.

## General Password Guidelines

The following standards have been set by the information security department and are thus strictly enforced without any exceptions.

* All users with user-level accounts, system-level accounts, web accounts, email accounts, local network log-in accounts, and corporate social media accounts will be prompted to change their passwords every 180 days. We highly recommend changing your passwords regularly, especially if you are working remotely.
* On the other hand, users with a privileged account to access systems and applications will be prompted to change their passwords every 90 days.
* Remote workers will be required to multi-factor authenticate to the company’s password-protected virtual private network (VPN) on devices before accessing BlackRock Inc.’s applications and systems hosted in the corporate network.
* Users who need escalated privileges to do their jobs should submit a ticket to the solutions center after getting their manager’s approval. Administrator teams will review the request and grant a temporary password with a limited life span to access systems or applications accordingly.
* All users are not allowed to use any of their previous five passwords to access resources. BlackRock’s password reset portals will highlight this information.
* The information security team might periodically perform password guessing or cracking on systems and applications. If successful, the account owner will be notified to change their password to be compliant with this policy.

## Policy Enforcement and Violations

* The standard and guidelines outlined in this policy are strictly enforced. Any violations of this policy can be reported risk and compliance team via email: [policyabuse@blackrock.com](mailto:policyabuse@blackrock.comt). Optionally, a web portal is also available on the company's intranet, where policy violations may be reported anonymously.
* Any employee, contractor, or related third party in violation of this policy or related international or local laws is subject to loss of access privileges pertaining to data, network, and computer privileges. Depending on the degree of violation, the individual might also be subject to disciplinary action and penalties ranging from a written warning to suspension, termination, or civil and criminal penalties accordingly (Whitman & Mattord, 2018).

## Limitations of Liability

* BlackRock and its related businesses are not held liable for the illegitimate storage and processing of the business information out of the guidelines stipulated in this policy and the associated legal penalties.

## Policy Review and Modification

* The guidelines stipulated are to be reviewed annually.
* The process of modification is to be performed by the policy administrator. The policy will then be reviewed by the CISO and a group of designated team members from the legal, human resources, and IT departments.
* Once the updated policy is approved, the team will create a plan to distribute and verify that employees, contractors, consultants, and other workers who own an account or are responsible for it, explicitly acknowledge that they have received and read the policy.

## Related Standards and Policies

* Criminal and Civil Laws
* Compliance standards such as SOX, GLBA, PCI-DSS, and GDPR
* BlackRock Inc.’s Acceptable Use Policy

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Responsible** | **Summary of Change** |
| 1.0 | 6/8/2020 | Natnael Kebede, CISO | Created the policy document. |
|  |  |  |  |

# 

# Appendix

## Policy Compliance and Auditing

The risk and compliance team collaborates with the information security department to verify compliance with this policy through various mechanisms. Note that any exceptions to this policy must be approved in writing by the information security department. Refer to the table below for more information on policy enforcement and auditing to achieve compliance.

|  |  |
| --- | --- |
| **Policy Element** | **Means of Enforcement/Auditing** |
| Remote access to corporate resources | Multi-factor authentication to the company’s password-protected virtual private network (VPN) application required. |
| Secure and robust password construction | Internal and external audit as well as through random checks of business systems reports by the risk and compliance team. |
| Create and utilize different passwords to access resources. | Utilize the Dashlane password manager application installed on devices to save, store, and recover passwords. |
| Avoid sharing your credentials and password with others | Once logged-in; all user activities are subject to monitoring and logging by the information security department. |

# References

BlackRock Incorporated. (2019). *2019 Annual Report*. Retrieved from https://s24.q4cdn.com/856567660/files/doc\_financials/2019/ar/BlackRock-2019-Annual-Report.pdf

Password Construction Guidelines. (2017). Information Security Policy Templates | SANS Institute. Retrieved from https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blta5be14c7136a535f/5e9dde89db124263e8afce3d/password\_construction\_guidelines.pdf

Password Protection Policy. (2017). Information Security Policy Templates | SANS Institute. Retrieved from https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt56ee6e15d78eb882/5e9ddf05d5a1cb709eee4a22/password\_protection\_policy.pdf

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security, 6th Edition [VitalSource Bookshelf version]. Retrieved from vbk://9781337671545