MFA and Password Guideline

Disclaimer These materials are internal BTC guidelines for awareness and consistency. They are not a contract, promise, or guarantee of specific outcomes. BTC may interpret, modify, or suspend this guidance at any time. Where law, partner requirements, or a signed agreement require different handling, that requirement controls. Questions or exception requests: support@bigthinkcapital.com.

Purpose Outline practical guidance for strong passwords and multi factor authentication. This is a guideline, not a mandatory policy.

Passwords - Aim for at least 12 characters using a mix of character types. - Prefer unique passwords for work accounts and avoid reusing personal passwords. - Consider an approved password manager if available. Avoid storing passwords in plain text. - If you suspect a compromise, change your password and contact support@bigthinkcapital.com.

MFA - Use MFA wherever it is offered, especially Microsoft 365, Salesforce, and RingCentral. - Prefer an authenticator app. SMS can be a backup when needed. - If you receive unexpected prompts, deny them and email support@bigthinkcapital.com.

Admins And Automation - Use separate accounts for administrative tasks when practical. - Store API keys and automation tokens securely. Rotate them periodically.

Exceptions If a team needs to deviate from this guidance, email support@bigthinkcapital.com with the context, risk, and temporary controls. Keep exception decisions in writing.