NAIGC Digital Account Access Policy

Version 1.0 / Last Amended: 5/1/2024

I. Purpose
   A. To provide a set of rules ensuring secure access to NAIGC accounts and organization login credentials on internet based services.

II. Individual Accounts
   A. Account access will be administered only on an as-needed basis, defaulting to minimum access levels until additional access becomes needed.
   B. Creation: requests for activating a new user account on services such as Google Workspace or the Password Manager shall be sent to the IT team when onboarding new employees or volunteers or when their needs change due to a new role.
   C. Deactivation: requests for deactivating a new user account on services such as Google Workspace or the Password Manager shall be sent to the IT team when offboarding employees or volunteers, or when their role no longer requires that they have access.
      1. The IT team should conduct an annual review of current account holders and deactivate any account access for volunteers no longer with the organization and activate any account access for volunteers who need it.
   D. No generic accounts should exist in Google Workspace or the Password Manager unless required. All generic email addresses such as treasurer@naigc.org, info@naigc.org, nationals@naigc.org etc shall be email groups within Google Workspace.

III. Organizational Accounts
   A. The NAIGC shall utilize a secure credential managing service to store account usernames and passwords. Credentials must not not be stored in any unencrypted format or service such as Google Drive.
   B. Where available, all accounts should have two factor authorization enabled.
   C. The department heads or team leads should notify the IT team of any access changes when they arise.
   D. Where applicable, organizational accounts which require a login email should use a non-personal group email, such as treasury@naigc.org or officers@naigc.org.
      1. Account passwords shall be changed at least annually or when someone with access is removed from that account.

IV. Credential Compromise
   A. Any user must report immediately to the IT team if they have a security incident or suspected security incident. This includes but is not limited to:
      1. Loss or theft of an electronic device which had their individual accounts, including personal accounts linked to NAIGC resources, or an organizational account logged in or saved on a browser.
      2. Software breaches such as viruses
   B. The IT team will immediately make appropriate remediations when a security incident is reported, including changing passwords, two factor keys, and/or disabling accounts, terminating remote sessions, as well as any other necessary measures.

V. Amendments

A. This policy may be amended by the NAIGC Board.

Document Revision History

Version/Date	**Author**	**Change/Reason**
Version 1.0 / 05/01/2024	Andrew Hutcheson, Kyle Thackston, Jimmy Koppel	Initial version