Privacy policy options for Firefox:

•        DisableAppUpdate :- Disables Firefox auto-update, which can prevent unnecessary data transmission to Mozilla

(For More information :- <https://mozilla.github.io/policy-templates/#disableappupdate>)

•        DisableFeedbackCommands :- Removes user feedback options related to deceptive sites or other issues

(For more information :- <https://mozilla.github.io/policy-templates/#disablefeedbackcommands>)

•        DisablePocket :- Disables the Pocket integration in Firefox(For more information :- <https://mozilla.github.io/policy-templates/#disablepocket>)

•        DisableFirefoxScreenshots :- Disables the built-in screenshot feature in Firefox(For more information :- <https://mozilla.github.io/policy-templates/#disablefirefoxscreenshots>)

•        DisableFirefoxStudies :- Disables Shield studies, which collect data for research purposes(For More Information :- <https://mozilla.github.io/policy-templates/#disablefirefoxstudies>)

•        DisableTelemetry :- Prevents the upload of anonymized telemetry data(For more information :- <https://mozilla.github.io/policy-templates/#disabletelemetry>)

•        OverrideFirstRunPage :- Overrides the page displayed when Firefox is run for the first time(For more information :- <https://mozilla.github.io/policy-templates/#overridefirstrunpage>)

•        EnableTrackingProtection :- Enables tracking protection to block trackers and enhance user privacy.

(For more information :- <https://mozilla.github.io/policy-templates/#enabletrackingprotection>)

•        OverridePostUpdatePage :- customizing the post-update page using this policy allows you to communicate privacy-related information directly to users, reinforcing a privacy-conscious browsing experience.

(For more information :- <https://mozilla.github.io/policy-templates/#overridepostupdatepage>)

•        Permissions :- Set permissions associated with camera, microphone, location, and notifications.

(For more information :- <https://mozilla.github.io/policy-templates/#permissions>)

•        Sanitizeonshutdown-all :- It will help in maintaining privacy as it will clear all the data when all the windows all closed of Mozilla.

(For more information :- <https://mozilla.github.io/policy-templates/#sanitizeonshutdown-all>)

•        PasswordManagerEnabled :- Remove access to the password manager via preferences and blocks about: logins.

(For more information :- <https://mozilla.github.io/policy-templates/#passwordmanagerenabled>)

•        PasswordManagerExceptions :- Prevent Firefox from saving passwords for specific sites.(For more information :- <https://mozilla.github.io/policy-templates/#passwordmanagerexceptions>)

•        ExtensionSettings :- Manage all aspects of extensions. This policy maps an extension ID to its configuration. With an extension ID, the configuration will be applied to the specified extension only. A default configuration can be set for the special ID “\*”, which will apply to all extensions that don’t have a custom configuration set in this policy.

(For more information :- <https://mozilla.github.io/policy-templates/#extensionsettings>)

•        EnableTrackingProtection :- It ensures that Firefox actively protects users’ privacy by blocking trackers and minimizing data exposure

(For more Information :- <https://mozilla.github.io/policy-templates/#extensionsettings>)

•        DisableFormHistory :- Turn off saving information on web forms and the search bar.

(For more information :- <https://mozilla.github.io/policy-templates/#disableformhistory>)

•        Cookies :- Configure cookie preferences to block third party cookies (For more information :- <https://mozilla.github.io/policy-templates/#cookies>)

**Additional Policies discovered:**

Current firefox settings are set to consumer settings. The Enterprise browser version needs to be replicated to mimic the privacy security policies similar to google chrome current settings.

Browser Privacy enabled to block Social Media trackers, Cross-site cookies in all windows, Tracking content in all windows, Cryptominers and Fingerprinters

Block pop-up windows enabled

Password breach alerts for websites enabled

Autofill – save and fill addresses and payment methods

Warning when trying to install add-ons

Secure and block dangerous downloads

Warn about unwanted and uncommon software

HTTPS-Only mode not ‘enabled’ (Provides a secure, encrypted connection btw firefox and websites visited. Most websites support https and if https-only is enabled then firefox will upgrade all connections to https)