Google Admin: Basic Workspace Setup

This checklist is designed to guide IT administrators in setting up Google Workspace according to best practices.

Following this checklist will help you optimize your organizational structure, keep it simple, manageable, secure, and ensure data protection.

0. Super-administration

☐ Assign Super Admin role to 1-2 key personnel for top-level management.
☐ Protect Super Admin roles with additional authentication mechanisms (keys/certificates).
☐ Use lesser privileged admin and non-admin accounts for regular activities.
☐ Review and audit admin roles regularly.

1. Organizational Structure

☐ Create an organizational structure in Google Admin Console.
☐ Define organizational units (OUs) for teams, departments, or business functions.
☐ Assign users to appropriate organizational units.
☐ Apply specific policies to each organizational unit as needed.

2. User Accounts, Roles and Permissions

☐ Create user accounts for all employees.
☐ Create user roles and set up roles security permissions based on job responsibilities.
☐ Assign users to their roles based on your organisational structure.
☐ Limit admin privileges to a minimal number of users.
☐ Regularly review and update user roles and permissions.

3. General Security Settings

☐ Enable two-factor authentication (2FA) for all accounts.
☐ Enforce strong password policies (e.g., length, complexity, and expiry).
☐ Set up alerts for suspicious account activity.
☐ Configure session timeout policies to automatically log users out after inactivity.

4. General Device Management

☐ Enroll all company devices (laptops, smartphones, tablets) in Google Workspace device management.
☐ Set up policies for lost or stolen devices (e.g., remote wipe).
☐ Require device encryption for all endpoints accessing company data.
☐ Ensure company devices have up-to-date antivirus and firewall software.

5. Data Access Control

☐ Configure access permissions for Google Drive, Docs, Sheets, and other services.
☐ Use shared drives for team collaboration with restricted access.
☐ Set expiration dates for file sharing with external parties.
☐ Regularly audit file sharing settings for sensitive data.

6. Email and Communication Security

☐ Enable email encryption (TLS) for secure communication.
☐ Set up email filtering for phishing and spam detection.
☐ Configure outbound email restrictions for sensitive data.
☐ Use Google Vault to archive emails for compliance and legal requirements.

7. Monitoring and Reporting

☐ Set up Admin activity logging in the Google Admin Console.
☐ Regularly review security reports and audit logs for unusual activity.
☐ Use the Security Dashboard for an overview of potential risks.
☐ Configure automated alerts for security incidents.

8. Training and Awareness

☐ Provide training for employees on Google Workspace best practices.
☐ Educate users on phishing and cybersecurity awareness.
☐ Create a policy document for acceptable use of Google Workspace tools.
☐ Encourage regular feedback on usability and potential improvements.

Need a hand with the next step?

If you have a question about any of these steps, or need help setting up a more advanced or tailored solution, we're here for you!

Feel free to send us an email at contact@403bits.com.

For simpler queries, we'll gladly share advice or point you in the right direction — free of charge!

And if you're facing a more complex challenge or want to save time, our experts can take over and deliver a comprehensive setup that perfectly fits your needs.

We're here to help you build security and efficiency
so you can focus on growing your business!

If you liked this checklist or have improvement suggestions, - let us know contact@403bits.com.