**Infrastructure & Technologies**

This document outlines the technologies to be utilized in the [company name].

**Planning**:

* **Jira**: A project management tool used for tracking progress, managing issues, and assigning tasks to team members throughout the software development lifecycle.
* **Microsoft Office**: Suite of productivity tools used for documentation, communication, and project planning.

**Design**:

* **Figma**: A collaborative interface design tool used for creating wireframes, mockups, and prototypes of user interfaces.
* **Draw.io**: Software for creating various diagrams such as flowcharts, org charts, and data flow diagrams.

**Development**:

* **Visual Studio Code**: A lightweight code editor used for writing and debugging code in various programming languages.
* **Visual Studio**: An integrated development environment (IDE) used for building, debugging, and testing software applications.
* **Postman**: An API testing tool used for creating and automating tests for APIs.
* **Jenkins**: An open-source automation server used for building, testing, and deploying software projects.
* **GitHub**: A platform for hosting and collaborating on code repositories using the Git version control system.

**Testing**:

* **Unit Testing**
  + **pytest**: A testing framework for Python that supports simple unit tests and complex functional testing.
  + **Mocha**: A JavaScript test framework running on Node.js, also used for browser-based testing.
  + **Jest**: A JavaScript testing framework developed by Facebook, often used with React applications.
* **Integration Testing**
  + **Pytest**: Python testing framework that supports integration testing.
  + **Postman**: Primarily used for API testing and supports integration testing.
* **System Testing**
  + **Selenium**: A tool for automating web browsers, used for end-to-end testing of web applications.
  + **TestComplete**: A functional test automation tool for desktop, mobile, and web applications
* **Security testing**
  + **Coverity**: A static analysis tool designed to identify security vulnerabilities and defects in source code. It scans the code for issues that can lead to security breaches and other problems, helping developers to fix them before deployment.
  + **CodeSonar**: A static analysis tool focused on identifying critical bugs that can affect security and reliability in the code. It provides deep static analysis by examining the entire codebase, including inter-procedural paths, to detect complex vulnerabilities.
  + **Snyk Code**: A tool that focuses on identifying and fixing vulnerabilities in the code by integrating with development workflows. It helps developers find security issues early in the development process, providing actionable remediation advice.
  + **Burp Suite:** A web vulnerability scanner that can perform both automated and manual scanning of websites to find vulnerabilities. It is a comprehensive tool for security testing of web applications, providing various features for identifying and mitigating security issues.
  + **Nessus:** A network vulnerability scanner that scans networks to detect vulnerabilities, misconfigurations, and compliance issues. It is widely used for vulnerability assessments and helps organizations strengthen their network security by identifying potential threats.
  + **Zed Attack Proxy (ZAP):** A web application security scanner that finds security vulnerabilities in web applications by acting as a proxy and intercepting and modifying HTTP/HTTPS traffic. It is an open-source tool used for security testing, helping developers and security professionals find and fix vulnerabilities in web applications.

**Deployment**:

* Jenkins: An open-source automation server that supports building, deploying, and automating any project.
* Azure DevOps: A set of development tools from Microsoft, including Azure Pipelines for CI/CD.
* GitHub Actions: Allows automation of workflows directly in GitHub repositories.
* Docker: A platform that automates the deployment of applications in lightweight containers.
* Kubernetes: An open-source system for automating the deployment, scaling, and management of containerized applications.
* OpenShift: Red Hat's Kubernetes-based platform for containerized applications.

**Collaboration and Communication Tools**:

* **Microsoft Teams**: A collaboration platform offering chat, video conferencing, and collaboration features for teams working on design projects.

**Hosting Services**:

* **Cloudflare**: A global network designed to secure, privatize, and optimize internet connections. Used for hosting web applications and ensuring traffic and security.
* **Microsoft Azure**: Provides a wide range of cloud computing services including computing power, storage, and databases.