templafy

SOC 3

Service Organization Control Report On Controls Relevant To Security, Confidentiality, And Availability

For Templafy Services

For the period January 1, 2024 through December 31, 2024

templafy

Table of Contents

templafy

Section I:

Independent Service Auditor's Assurance Report Provided By Diggle

Independent Service Auditor's Assurance Report Provided By Diggle

To The Templafy Board of Directors

Scope

We have examined the management of Templafy's (the "Service Organization") accompanying assertion titled "Templafy's Management Assertion" (the "assertion") that the controls within Templafy's system ("system") were effective throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality ("applicable trust services criteria") set forth in the 2017 edition of TSP Section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (with Revised Points of Focus – 2022)* issued by the Assurance Services Executive Committee of the AICPA.

Templafy uses Microsoft Azure as a cloud platform and datacenter service to host its services ("subservice organization"). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at Templafy, to achieve Templafy's service commitments and system requirements based on the applicable trust services criteria. Our examination did not extend to the controls implemented by subservice organizations.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Templafy's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

Service Organization's Responsibilities

Templafy is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Templafy's service commitments and system requirements were achieved. Templafy has also provided the accompanying assertion in section II titled "Templafy's Management Assertion" (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. When preparing its assertion, Templafy is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior. We applied the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA – RKBN), and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Templafy's service commitments and system requirements based on the applicable NOREA Guide SOC 2® and SOC 3® reports
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Templafy's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Service Organization's system were effective throughout the period January 1, 2024 to December 31, 2024, to provide reasonable assurance that Templafy's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

On behalf of Diggle B.V.,

Drs. C. Meulendijks RE

Partner Diggle B.V.

Eindhoven | January 15th, 2025

templafy

Section II:

Templafy's Management Assertion

Templafy's Management Assertion

We have prepared the accompanying description around the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality. The description is intended to provide report users with information about the Templafy Services that may be useful when assessing the risks arising from interactions with Templafy throughout the period 1 January, 2024, to 31 December, 2024, particularly information about system controls that Templafy has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, confidentiality and availability set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable Trust Services Criteria).

We have prepared the accompanying description based on the criteria of a description in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report® (AICPA, Description Criteria) ("description criteria"). We confirm, to the best of our knowledge and belief, that:

1. The accompanying description in section III fairly presents the Trust Services Criteria of Security, Confidentiality and Availability in relation to Templafy's service used by customers throughout the period January 1st , 2024, to December 31st, 2024. The criteria used in making this assertion were that the accompanying description:
    i) Presents how the system was designed and implemented, including:
        - The types of services provided,
        - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary and transferred to the reports prepared for customers,
        - Relevant control objectives and controls designed to achieve those objectives,
        - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone,
        - How the controls dealt with significant events and conditions, other than transactions,

- Other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.

ii) Includes relevant details of changes to our control systems during the period January 1st, 2024, to December 31st, 2024.

iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.

2. The controls related to the control objectives stated in the Templafy description were suitably designed and operated effectively throughout the period January 1st, 2024, to December 31st, 2024. The criteria used in making this assertion were that:

   i) The risks that threatened achievement of the control objectives stated in the description were identified;

   ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

   iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period of January 1st, 2024, to December 31st, 2024.

On behalf of Templafy,

Ellen Benaim

CISO

Copenhagen | January 15th, 2025

templafy

Section III:

Description Of The Boundaries Of The Templafy System

The Templafy Organization

System Overview and Background

Templafy Inc. (Templafy), headquartered in the United States, is a business enablement Software-asa-Service (SaaS) platform that provides document creation, collaboration, productivity and email signature tools (Services) for users of Microsoft Office and Google Suite, supporting every step of the document creation workflow. Templafy was founded in Denmark in 2014 and has been fast-growing since, with employees in Denmark, the USA, The Netherlands, Germany, the UK and Australia. Templafy is committed to achieving and maintaining the trust of its customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across the suite of Services by design and default, including data submitted by customers to the Templafy Services. Templafy's enterprise customers span most industries globally, such as banking, financial services, professional services, industry, health, education and governmental. Both Templafy and its Services are crafted to meet their security, confidentiality and compliance requirements. Templafy is a multi-tenant SaaS platform. Each organization that uses the Templafy Services shares a set of resources. The main interaction point for end-users is the Templafy web application and the Templafy add-ins. Add-ins are provided via Application Programming Interfaces (APIs) and add-in models by Microsoft and Google. Furthermore, Templafy integrates into or with Document Management Systems, Customer Relationship Management (CRM) solutions, Digital Asset Management (DAM) solutions and Enterprise Resource Planning (ERP) solutions via APIs.

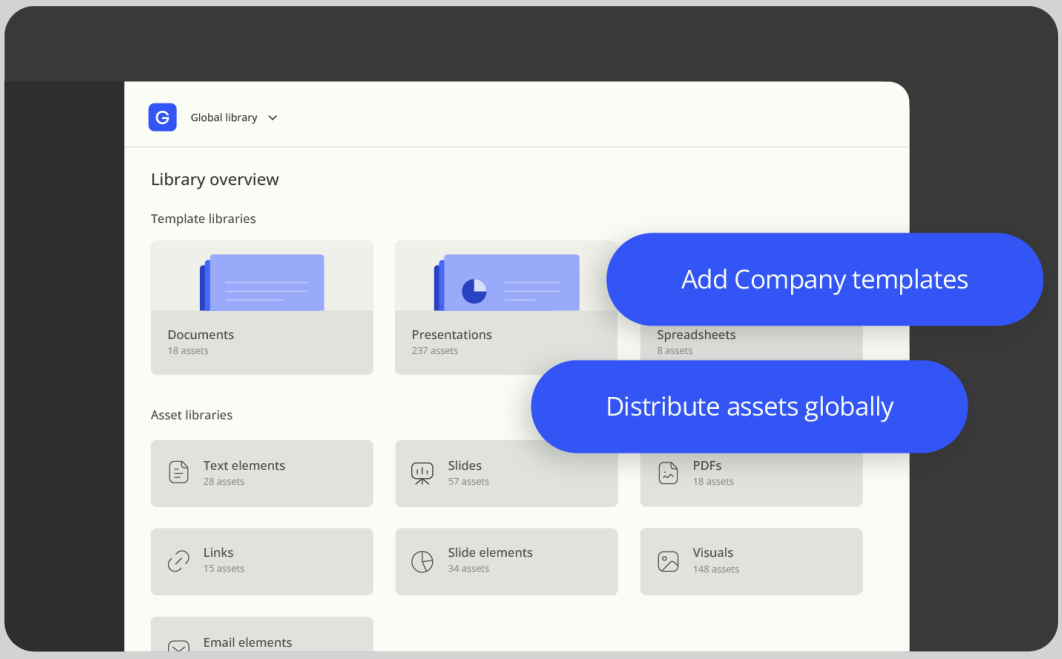

Figure 1 - Templafy User Experience

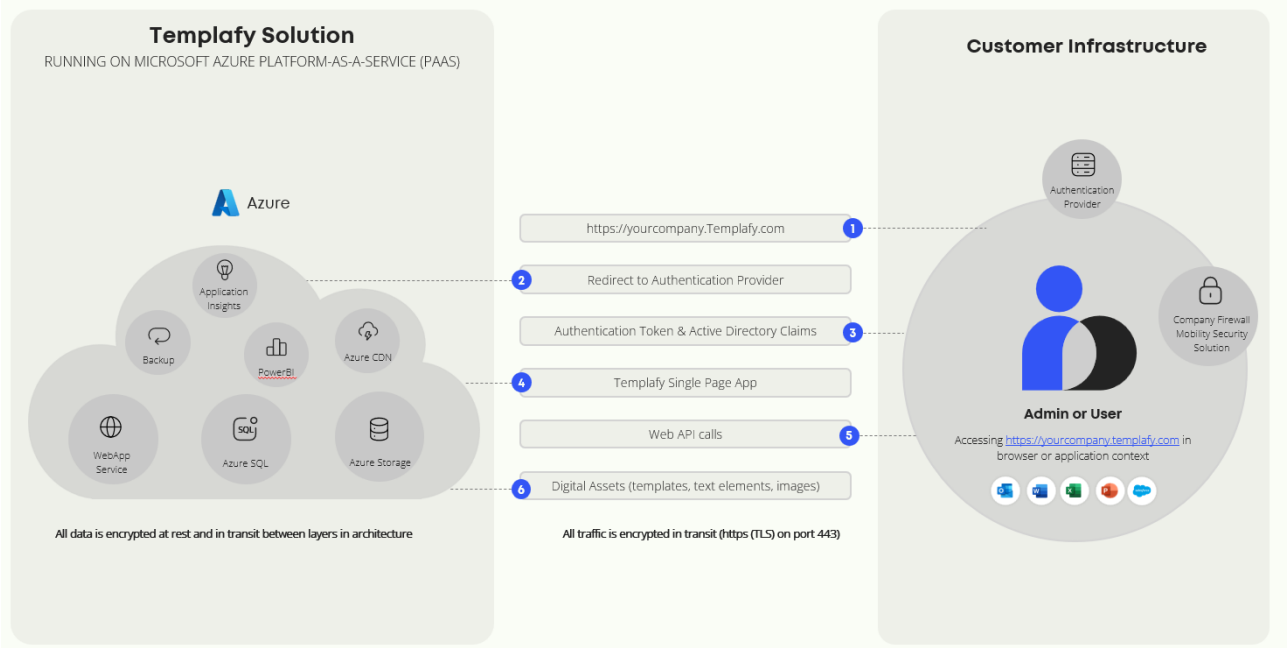

Figure 2 – Templafy Single sign-on and Data Flow

Description Of Covered Services

The scope of this report covers the Templafy Services described in Figure 4. Templafy provides various tools to enable professionals to create better performing documents faster through connected content.

	Service Name	Service Description
Platform	One	Real-time management and distribution of document templates and digital assets. Filtering and access management with filters and AI (Artificial Intelligence) powered tags. Role-based access control (RBAC) of user access rights throughout the platform. Add-ons to content distribution: • Font Distributor distributes and manages fonts across the whole organization for font control. • Offline content distribution. Integrations management: • DAM integration • CRM integration • DMS integration
	Hive	Templafy Hive is the second iteration of the platform. Templafy moved from a monolithic architecture to a microservices architecture and structured our software in separate, connected units. Real-time management and distribution of document templates and digital assets. Filtering and access management with filters and AI powered tags. Role-based access control (RBAC) of user access rights throughout the platform. EU data protection access filter and activity log available to customer admins. Add-ons to content distribution: • Font Distributor distributes and manages fonts across the whole organization for font control. • Offline template distribution and access.

		• Spaces for content libraries to manage and distribute document templates and digital assets in real-time management to a specific group. Integrations management: • App connector (e.g., Office applications, Office 365, Salesforce, G-Suite, Teams). • Data connector (e.g., Salesforce, Highspot and other company data sources). • Content connector (e.g. Bynder, Aprimo and other company DAM solutions). • Delivery connector (e.g., SharePoint, Highspot and other company DMS solutions).
Modules	Library	Direct access to the latest business document assets like slides, graphs, text elements, images etc. through a userfriendly task pane add-in inside document creation applications. Filtered access to relevant assets based on user profile and office location. Integrate and connect with company image banks and digital asset management applications to bring all the relevant assets close to the user (optional).
	Dynamics	**Templates**: Building, updating, and maintaining automatically personalized templates with brand and compliance information through dynamic content fields. **Metadata**: Dynamically inserted metadata and data loss prevention (DLP) information **Compile**: Building, updating, and maintaining complex documents like sales quotes, contracts and quarterly reports becomes an easy task.
	Validator	Chosen PowerPoint presentations validated against up-to date latest versions uploaded in Templafy. Easy

		update of reused presentations through a simple popup appearing right in PowerPoint.
	ProductivityPlus	Pro-presentations made easy using intuitive features designed to build complex slides while making professional formatting simple. Import and link tables, data cells, and graphs from Excel to PowerPoint with a simple copy-paste. Keep the linked data up to date with real-time update function.
	Check	Check function inspects documents against up-to 40 pre-defined rules and ensures that the content, format, and layout are professional. Fix format, layout, and content compliance issues fast with one click before sending. Get an overview of issues in the Templafy task pane and use the Fix button to quickly amend the presentation.
	Email Signature Manager	Unified look and feel for all email signatures for enterprise-wide use, and support for multiple signatures per user. Management of multiple brands and office locations in one dynamic layout through our easy-to-use centralized platform. Real-time roll out and updates of email signatures and seasonal campaigns. Email signatures for Outlook Online, Windows, Mac and Mobile. Email signature servers hosted by Templafy or clients themselves. Add on: Advanced mobile signature hosting solution for no rerouting of emails outside of company servers with self-hosting.
	Engage	*Only available on Templafy Hive platform* Document sharing embedded into the organic workflow of every employee. Curated collaboration workflows optimize the approval process, contract negotiations and co-creation. Document insights

		dashboard with actionable data transforms every business document into performing one.
	AI Assistant	Universal AI assistance when writing, elaborating and curating text within the workflow of employees while not compromising on governance and control. The AI text assistant is embedded into employee workflow within document creation applications and allows to centrally manage tones of voice of the AI output and prompts available for end users.

Figure 3 - Templafy Services

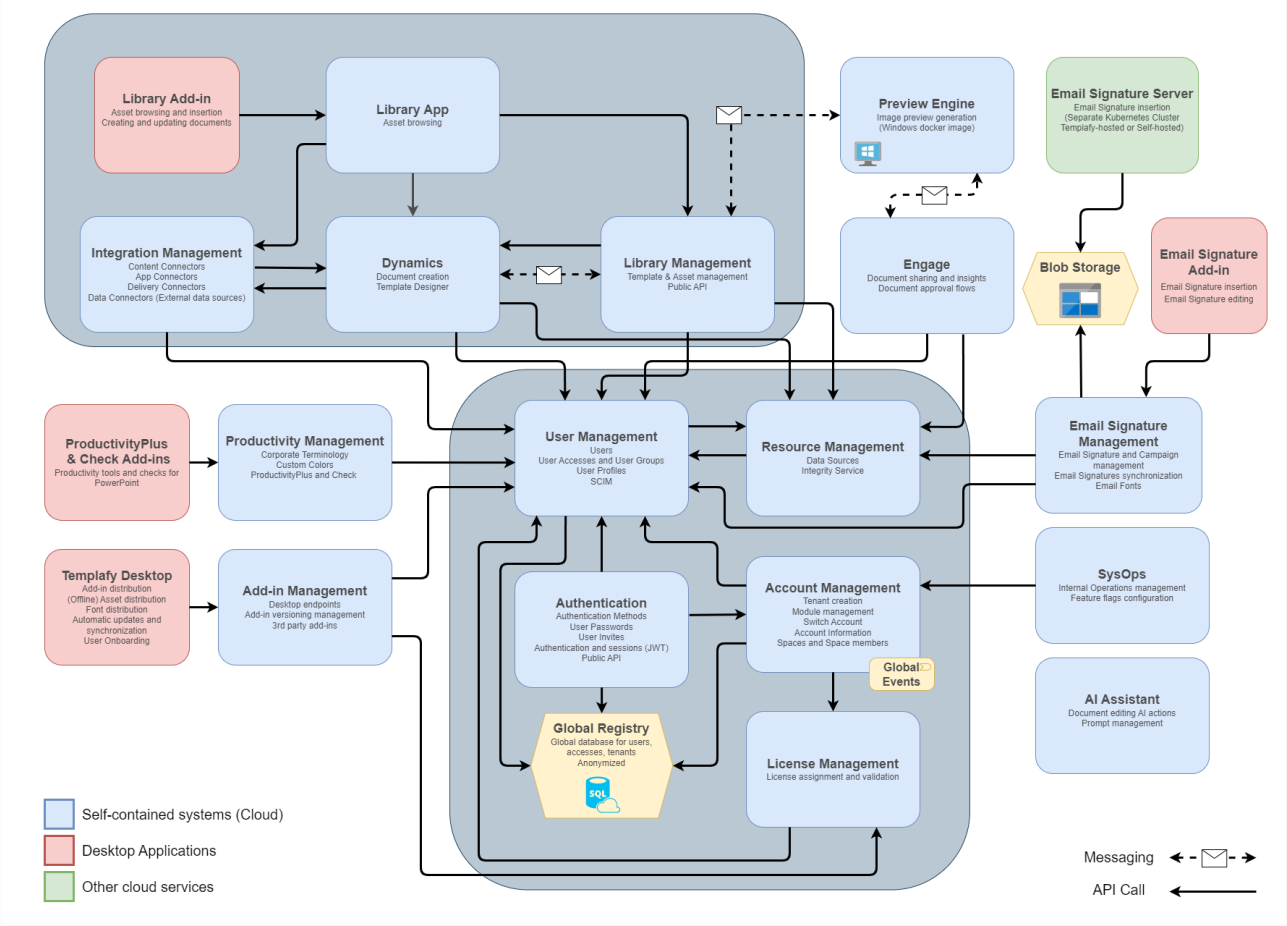

Figure 4 - Self-Contained System Architecture

Components Of The System Providing Services

Overview Of Templafy Architecture

Templafy Services are operated in a multi-tenant architecture that is designed with tenant isolation to segregate and restrict customer data access based on business needs. The architecture provides logical data separation for different customers via customer-specific unique identifiers (IDs) and allows the use of customer and user role-based access privileges. This is done on every request and background job when connecting to the database and storage accounts. Templafy Hive consists of self-contained systems (also known as microservices). Each self-contained system is built using the same foundation (.NET) with strong operational consistency. The foundation is developed by a platform team that ensures that no product teams (or individual engineers) are responsible for the segregation of customer data.

Each self-contained system runs in a docker container hosted in Azure Kubernetes Service (AKS) to support millions of daily users. Templafy uses Infrastructure-as-Code with a focus on security and DevSecOps techniques. Self-contained systems running in Kubernetes access the database using Managed Identity. Managed Identity is an Azure solution that allows one service to securely access and communicate with another service without needing to remember or share any passwords. Other than self-contained systems, only a selected number of users (Site Reliability Engineering Admins) can access the database using Azure Entra ID Accounts, where MFA is required for these accounts. Additional data segregation is maintained by providing separate environments for different functions, including for testing and production. Product functionality and system architecture are designed with security by design and default.

Infrastructure	
Function	**Description**
Public Cloud Service Provider Microsoft Azure	**One** North Europe (Primary) and West Europe (Secondary) **Hive** West Europe (Primary) and North Europe (Secondary) East US (Primary) and West US (Secondary) Australia East (Primary) and Australia Southeast (Secondary) Central Canada

Data Analytics Platform	West Europe (Primary) and North Europe (Secondary)
AI Assistant and AI Data Transformation	Based on Hive storage selection: Sweden Central (for customers who opt for storage in Europe) East US (for customers who opt for storage in the US) Australia East (for customers who opt for storage in Australia) Canada East (for customers who opt for storage in Canada)
Software	
Function	**Description**
Operating System	• Kubernetes • Linux • Docker • Windows Server
Databases	Microsoft SQL Server and Databases
Monitoring Systems	There are multiple monitoring systems in use, including: • Azure Monitor • Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Storage • Azure Security Centre • Advanced Threat Protection • Azure Application Insights • Azure Container Insights • Azure Sentinel • WhiteHat Security • SonarCloud • Ontinue

Network Infrastructure	Templafy Services' network infrastructure utilizes a common set of network components, including: • Azure Load Balancer • Azure Firewall • NGINX • Azure Virtual Network • Network Security Group
Core Systems	Microsoft Azure • Azure App Services • Azure Kubernetes Service • Azure Key Vault • Azure CDN • Azure Cognitive Services Azure Storage Accounts • Azure Network Watcher • Azure Service Bus • Azure Data Lake • Azure DNS Amazon Simple Email Service (SES) SendGrid Azure DevOps
Supporting Systems	Dashlane PagerDuty StatusPage Zendesk Slack One Trust
Endpoint Protection	Microsoft Intune Microsoft Defender for Endpoint Defender Advanced Threat Protection BitLocker Windows Firewall

	FileVault (macOS) Apple Firewall (macOS) Admin By Request

Figure 5 - Infrastructure and Software Components

People

Templafy's structure is documented in its organizational chart, which shows the separation of duties and levels of oversight. The CEO leads the company, and there are multiple C-Suites who report to the CEO. Templafy has a board of directors overseeing its governance. Templafy's board of directors is comprised of representatives that are independent of management. The following teams are in-scope as their job responsibilities require that they have access to production systems, develop code to be included in the environment or supporting operational and advisory functions:

Department	Responsibilities Covered (Non-Exhaustive)	Office Location
Engineering	Change, development, security and availability responsibility over Templafy Services	Copenhagen Berlin Eindhoven London
Technical Operations	Deliver and support to customers	Copenhagen Berlin Eindhoven New York Sydney
Information Security	Security and privacy over Templafy Services and Templafy	Copenhagen
IT	Provision and manage employee laptops and desktops Mobile device management Network management	Copenhagen New York

Customer Success	Enable the customer usage of Templafy Services	Copenhagen New York
Product	Strategic direction and prioritization of Templafy Services roadmap	Copenhagen Berlin Eindhoven
People+	Onboarding/offboarding employees Employee background checks Performance management	Copenhagen Berlin Eindhoven New York

Figure 6 - Templafy Departments

Processes and Procedures

Templafy has implemented an Information Security Management System (ISMS) based on the International Organization of Standards (ISO) Codes of Practice for Information Security Management ISO IEC27000:2017 standard (ISO 27001:2022 and ISO 27017:2015). Templafy chooses to focus on the highest quality level of controls to achieve a risk-based approach in preserving the confidentiality, integrity and availability of information. Organization-wide, Templafy is committed to continually improving the suitability, adequacy and effectiveness of the ISMS. Templafy has extensive information security policies and procedures pertaining to confidentiality, integrity and availability, such as:

- Information security
- Risk management
- Access control
- Physical and environmental security
- Personnel security
- Awareness and training
- Asset management
- Cryptography
- IT operations
- Network and information transfer
- Software development lifecycle
- Change management
- Vulnerability management
- Supplier risk management
- Incident response management
- Business continuity and disaster recovery
- Privacy policy

Data

Customer Agreements

Customer data means electronic data and information submitted by or for the customer to the Templafy Services as defined by the publicly available Templafy General Terms and Conditions

Agreement (SaaS agreement). Templafy has an information classification procedure and has classified customer data as restricted, the highest level. Templafy complies with privacy standards and is governed by a data processing agreement to ensure the data receives the appropriate level of protection. Customers are covered under Templafy's data processing agreement available on the website unless a contract is otherwise entered. Templafy retains and disposes of customer data in a secure manner in accordance with customer agreements and information classification and handling procedures. Customer data is disposed 90 days after termination of customer contract, and as soon as possible for active customers requesting specific data removal.

Customer Data Elements

Templafy stores public enterprise information such as office locations and legal disclaimers, digital assets (such as office templates, email signatures, text snippets, images for image library, icons). All these digital assets that are provided by customer admins are then uploaded into the system. Digital assets are stored in a unique Azure Blob storage for each customer. Validation checks are performed upon files upload and restrictions to certain file types are enforced. Content length limit is in place for all requests. Input validation is applied on the front-end with property size check (e.g., string length, valid email address) before the back-end APIs are called. Back-end checks ensure full validation on domain layer and database layer. Contact information about employees such as name, job title, work email, work phone numbers and work location are stored to personalize the templates used. User profile information is stored in a logically segregated SQL database. Users are authenticated based on customer admin selected authentication method. Customer admins determine which user profile data elements are processed by Templafy and modifiable by customer end-users. Templafy supports just-in-time (JIT) provisioning, single-sign on (SSO), multi-factor authentication (MFA), and on-boarding against customer Active Directories (AD).

Templafy Data Flow

Users access Templafy in the web application or application add-in (e.g., Word, PowerPoint). Add-ins are provided via Application Programming Interfaces (APIs) and add-in models by Microsoft and Google. Templafy also integrates into or with DMS, CRM solutions, DAM solutions and ERP solutions via APIs. APIs are subject to vulnerability scans and penetration testing. A user starts the document generation flow by selecting a template file in the web application or application add-in. User profile information is retrieved from the SQL database and added to the template to personalize it as directed for the user. Templates may have gating questions' answers injected into it as configured by customer admins, which the user can answer through a form interface. Templafy connects the template, any user profile information, data source information and the answers to the gating questions in a background

job. The data filled template is permanently deleted after twenty-four hours from the unique temporary blob storage which is required to perform the injection. The end-user receives a read-only shared access signature (SAS) download link valid for a few minutes, where the final template is generated onto the local machine. The SAS link facilitates secure communication when data is stored in the blob storage. The connection to Templafy ends here. The user can then use the data filled template to build further to the document or presentation, which is not stored back to Templafy. The file is shared on the customer's own local or cloud DMS. All requests throughout the document generation process are encrypted in transit and valid authentication of the user is required. Microsoft Defender is used to detect unusual and potentially harmful attempts to access or exploit storage accounts which are sent to our SIEM tool to be handled according to our incident management procedures described in the incident management section. HTTPS is always required to access the storage account, including for the SAS link. This flow can only be triggered if the end-user is authenticated to Templafy. The data flow diagram is available upon request.

Relevant Aspects Of The Control Environment, Risk Assessment, Information And Communication, Monitoring

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), this section provides information about the five interrelated components of internal control at Templafy:

- Control Environment. Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Risk Assessment. The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.
- Control Activities. The policies and procedures that help make sure that management's directives are carried out.
- Information and Communication. Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Monitoring. A process that assesses the quality of internal control performance over time.

Control Environment

Organizational Structure And Assignment Of Authority And Responsibility

The board of directors and executive management play an integral role in demonstrating from the top the importance of security, including integrity and ethical values throughout the organization. Information security is seen as a key strategic initiative, therefore the Chief Information Security Officer (CISO)reports once a year to the board of directors and frequently to the management team. . The CISO is head of the information security department. The information security team implements the Information Security Management System (ISMS) and provides security guidance throughout the organization

Chairman of the Board of Directors: The Chairman of the Board of Directors oversees information security overall, sets strategic direction and assigns priority to support the information security objectives in Templafy. They allocate investment in alignment with the organization strategy and risk profile. They review Templafy's information security program's adequacy and effectiveness on a frequent basis. They have oversight of strategic security risks and provide prioritization and advisory.

Chief Information Security Officer: The Chairman of the Board of Directors and Management Team have appointed a Chief Information Security Officer (CISO). The CISO is overall responsible for designing, implementing and monitoring a strategic, comprehensive Templafy-wide information

security strategy aligned to the overall organization strategy. The CISO is a member of the Management Team and reports directly to the Chairman of the Board of Directors. The CISO reports to the Board at least annually. The CISO appoints and manages the Information Security department.

Management Team: The Management team endorses and supports the development and implementation of a comprehensive information security program and its components. They review the status and impacts of security initiatives and act appropriately on management reports concerning information security performance metrics, security incidents and risks, investment requests, policy exceptions etc. The Information Security department's budget is approved in line with the budget process set by the Management team.

Information Security Department: The Information Security department acts as a design and operational function, and the members work with various business units and other operational entities to implement a consistent and Templafy-wide information security program. The Information Security department are responsible for defining technical and non-technical information security standards, procedures and guidelines and supporting Templafy leaders and employees in the definition and implementation of controls, processes and supporting tools to comply with the information security policies and manage information security risks.

Leaders: Leaders must ensure their employees are informed of their obligations to fulfil the Information Security Policy where relevant to their roles and lead by example in respective departments. Leaders must actively support the associated information security objectives and initiatives by providing the direction, resources, support and reviews necessary to ensure that information assets are appropriately protected within their area of responsibility. Leaders must monitor compliance and remind users of their obligations and escalate non-conformities as required. Management communicates and oversees the requirements regarding conduct, professional integrity, and ethics by making the code of conduct available in Templafy's internal SharePoint site and through documents signed by employees.

Personnel Security

Awareness training: Templafy has a strong security-first mindset due to repeated emphasis and communication around numerous security topics to all the organization on a frequent basis. Templafy has put in place security awareness initiatives and a training awareness program. All employees and contractors receive information security awareness training at onboarding, and at least annually thereafter. The security awareness training covers information on relevant security best practices and includes the responsibility for every employee and contractor to communicate security concerns. Job specific training is provided to personnel where appropriate. Awareness is raised with weekly security

updates in town hall meetings, communication efforts via email, and internal communication tools. New employees are required to review and acknowledge their receipt of the Information Security Policy, Acceptable Use Policy, and Information Classification and Handling Policy during onboarding. Confidentiality and intellectual property rights classes are included in employment contracts. Once employed, employees are subject to Templafy's procedures and sanctions for violating Templafy's information security policies.

Onboarding and offboarding: Templafy has a process for revoking system and building access and returning assigned assets. This is integrated into the onboarding and offboarding process within the Human Resource (HR) system. The task to revoke system and building access are assigned to responsible individuals and are completed in a timely manner. The People+ and IT team is responsible for ensuring the onboarding and offboarding tasks are completed correctly and within stated time intervals. For a change of roles or position change, an automatic alert is generated from the HR system to the information security team and based on this alert, a review is conducted as to the appropriate levels of access. Subsequent action is taken based on the review. Periodic access reviews are conducted as described in the logical security section.

Background checks: Background checks are performed on new employees, before they start at Templafy, who will have access to the production environment or production data, as permitted by local laws. Candidates are evaluated against documented job descriptions that define the skills, responsibilities and knowledge levels required for all critical roles in the organization. Due to local restrictions in Germany and The Netherlands, a criminal record check cannot be performed in these countries, however; a criminal conduct search is performed instead. The background checks performed include identity verification, employment verification, professional reference checks and criminal record check. In the United States, a criminal felony and misdemeanor search within the last seven years is carried out.

Disciplinary process: A process and submission form are in place to facilitate anonymous notification of inappropriate behavior, including non-compliance with the Information Security Policy and its supporting standards. A formal disciplinary action process is enforced for personnel failing to comply with the established Information Security Policy and standards, where all reports of non-compliance are investigated by the People+ team, information security team, and other department representatives as required, through to resolution.

Risk Assessment

Templafy has established an organization-wide information security risk assessment process to identify and manage information security risks across the organization. It enables Templafy to identify, evaluate, and mitigate the risks that may threaten the achievement of its service commitments and system requirements related to security, availability, and confidentiality based on the applicable trust services criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Templafy performs an annual risk assessment that covers security, privacy, continuity and operational risks. The risk management process is derived from ISO 27005 and aligned with the COSO 2013 framework. As part of this process, threats to security are identified, and risks from these threats are formally assessed. Security risks related to external parties (such as customers, contractors, sub-processors and suppliers) are identified and addressed. The assessments include threats, vulnerabilities, impact, likelihood and mitigating controls. Following the risk assessment, a risk treatment plan is implemented to mitigate risks. After the treatment plan is evaluated and residual risk rating obtained, acceptance is obtained from risk owners. Changes in security threats and risks are reviewed by the information security team, and updates to existing control activities and information security policies are performed, as necessary. The CISO, as part of the annual management review of security, considers developments in technology and the impact of applicable laws and regulations to Templafy's security policies. The chairman of the board of directors receives reports on a quarterly basis covering the main ongoing risks and the management review report on security at year-end.

Control Activities

Software Development Lifecycle

Templafy has a Secure Development Lifecycle (SDLC) methodology across each of the engineering teams, aligned with the best security standards such as ISO/IEC 27001, and follows Scrum and Agile approaches. Detailed policies and processes for the development of the Templafy Services have been designed with optimal security and quality in mind. The principles of security by design and default are implemented and rooted in training, coaching, pair programming, code review comments, coding tools and branch policies in Azure DevOps. Templafy has implemented segregated environments for development, test and production as a means to support segregation of duties and prevent unauthorized changes to production. In addition, production data is not used or copied to non-production environments. Test scripts and synthetic data are created for use in the development and staging environments.

Change Management

Changes are prioritized in collaboration with product owners and engineering teams. Information security and availability considerations are core components in application development and testing. Project management frameworks are used to manage application development and testing, and roles and responsibilities are identified throughout the system development lifecycle.

Azure DevOps is used to plan, schedule, approve, apply, distribute and track changes to the production environment with designated responsibilities and enforced through branch policies. It controls the integrity and reliability of the environment while maintaining a continuous delivery model without downtime.

All application code changes are tested, peer-reviewed and approved prior to implementation into production. The production and non-production environments are deployed in their own Azure Active Directory and their own Azure Subscriptions, thus completely separated, and changes are tested according to the nature of the change in an environment separate from production prior to deployment into a production release. Tests include functionality unit testing, integration testing, smoke tests, manual regression testing and load testing. Extensive security testing is conducted (see vulnerability management section).

All change requests are logged, whether approved or rejected, on a standardized central system. The approval of all change requests and the results thereof are documented. Access to migrate change to production requires formal approval and is restricted to authorized personnel. Code management tools enforce branch protection policies to help ensure users cannot bypass standard change controls. The Product Owner and the engineering team discuss the status and progress of all outstanding changes within the current sprint during daily stand-ups. Release notes are documented and communicated to internal and external users via the knowledge center for changes related to feature and security changes.

Templafy maintains a continuous delivery model of the Services. Patch management is incorporated into the SDLC to ensure necessary updates, fixes and other changes are timely implemented to the Services. Patches are released like any other change in Templafy's SDLC and follow the same change management procedures. Patch implementation timescales are defined to ensure timely patching in accordance with severity. Different automatic release plans are made available to customers to choose from newest software features for testing purposes or stable and most reliable versions.

Baseline Configuration Hardening

Templafy's security configuration standards are applied through automated deployment mechanisms to help ensure consistent application. Templafy uses secure OS configurations deployed via Kubernetes. Templafy leverages hardened Azure Public Compute Images for servers. Templafy continuously monitors all resources deployed in the Azure environment in conformity to Azure best practices, CIS, ISO27001 and SOC 2 compliance requirements and applies applicable recommendations after review by the security guild.

Infrastructure As Code

Templafy implements Infrastructure as Code (IaC) to streamline the deployment and management of its infrastructure through programmable scripts and configuration files. By using Terraform, Site Reliability Engineers define and provision infrastructure elements automatically. IaC enforces consistent security configurations across all environments ensuring that security controls and best practices can be codified and applied consistently, reducing the risk of misconfigurations or human errors that could lead to vulnerabilities. This includes encryption protocols, access controls, firewall rules, and monitoring configurations. Security configurations are applied uniformly across development, testing, and production environments, bolstering the overall security posture of the Templafy product.

Encryption

Templafy has implemented best practices regarding encryption methods and has implemented a secure process for transmitting or receiving data across open, public networks.

- Templafy One and Hive support TLS1.2.
- Data at rest is encrypted using AES 256-bit encryption is enabled by default throughout all Azure services in use for the Templafy Services.
- TLS1.2 is used to communicate between all the Azure services in use for the Templafy Services.
- File and disk level encryption on blob storages.
- Disk level encryption on SQL database.

The transmission, movement, and removal of information are restricted to authorized internal users and processes.

Authentication towards our Azure native PaaS services is done through Azure managed identities. The key management of Service-Managed keys for data at rest encryption is performed by Azure. The certificates used for data in transit encryption are managed using Azure Key Vault by Templafy and are subject to Templafy cryptography policy.

Vulnerability Management

Templafy has a vulnerability management process in place to discover, assess, remediate, and track vulnerabilities in Templafy services and supporting infrastructure. A risk assessment is carried out on the discovered vulnerabilities and a risk rating is assigned to prioritize the remediation accordingly. The vulnerability remediation is documented in the work item in DevOps and the changes required are carried out in-line with Templafy's change management procedures as described in the change management section. Vulnerabilities are classified into 4 different levels: informational, low, medium, high based on their impact. The impact is determined by the threat level, the risk of compromise and the consequences of compromise.

Open-source: Templafy only uses developed and tested open-source libraries to enhance our product offering. We have a central repository of dependencies and whitelist of approved dependencies and versions. Templafy continuously scans and tracks 3rd party dependency risks and report findings through our vulnerability management flow internally and back to dependency authors for remediation using Snyk. Templafy constantly updates all our 3rd party dependencies. We use a tool called Renovate to ensure that any security or bug fixes are applied without delay. We manually review licenses for new 3rd party tools. Despite not being often, any new 3rd party dependencies go through a due diligence procedure.

Penetration Testing: Penetration testing is conducted to measure the security posture of the Templafy Services and Infrastructure. Templafy has an external penetration test performed at least once per calendar year. The objective of those penetration tests is to identify design or functionality issues in Templafy Services that could expose Data or Customer to risks from malicious activities. Each external penetration test is performed by an internationally recognized, independent third-party software security testing company. Each penetration test (i) encompasses both the internal and external network and authenticated application layer, (ii) includes at least 80 hours of manual effort by the testing company, (iii) probes for weaknesses in network perimeters or other infrastructure elements and any weaknesses in process or technical countermeasures relating to Templafy's Services that could be exploited by a malicious party, and (iv) identifies (at a minimum) the following security vulnerabilities: invalidated or unsanitized input; broken access control; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; denial of service; insecure configuration management; proper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.

Customer-led penetration testing can be conducted upon request to the information security team and is subject to conditions prior to carrying out the tests.

Vulnerability Scanning: Vulnerability scanning is performed on a continuous basis by Templafy in accordance with the vulnerability management policy. Technologies used are:

- WhiteHat Security scanning for 24/7 web application dynamic application security testing (DAST),
- SonarCloud for static application security testing (SAST) before each release
- Renovate for ensuring that open-source dependencies always are the latest available version
- Snyk for software composition analysis (SCA).
- Azure Security Center and Azure Monitor for daily infrastructure, network and application vulnerability scanning. Retests and on-demand scans are performed on an as-needed basis.

Alerts And Results: Anomalous user behavior is captured through user behavior analytic (UEBA) tooling. Centralized data loss prevention (DLP) solution is implemented as protection against data leakage. The information security team is responsible for continuous monitoring and reacting upon alerts from numerous rules from these technologies, feeding into centralized reporting dashboard. Individual vulnerabilities identified during penetration and vulnerability testing are logged to the appropriate change management software and managed through the vulnerability management process. Scan and test results are assessed by the security and engineering teams, risks for each vulnerability are identified, and remediation is approved and prioritized until resolution in a timely manner. Vulnerability reports include a client summary, which is available to Templafy's customers upon request.

Security Operations Center

Templafy has implemented a Security Operations Center (SOC) to mitigate threats and reduce risks to its internal infrastructure.

The Security Operations Center (SOC) functions as a provider of Managed Detection and Response (MDR) services, ensuring round-the-clock 24x7 monitoring, detection, and response to threats. This is accomplished by utilizing a blend of technologies deployed at both the host and network levels, alongside advanced analytics, automated response protocols, threat intelligence, and expert human intervention. Once confirmed positives are identified, the MDR service's capabilities extend to executing the necessary response procedures outlined in our Incident Management procedures. Moreover, our SOC furnishes supplementary threat intelligence functionalities to enhance daily security operations, uncovering novel, enhanced, or unfamiliar attacker methodologies, including zero-day exploits. Alerts are aggregated in a dashboard that provides a concise overview of operational performance and grants visibility into security incidents. Additionally, we regularly receive comprehensive Security Operations

summaries in the form of quarterly Action Reports, offering insights and recommendations pertaining to Templafy's security program.

The SOC uses automation to perform initial triage and to trigger an Automated Investigation and Response (AIR) in Microsoft Defender Initial assessment involves scrutinizing each incident, resulting in either closing it as a benign positive or escalating it to a Cyber Defender for further examination. Incidents are closed directly within Sentinel, and comments made during investigations are updated within the Sentinel incident. The Automated Investigation and Response intercepts threat actors early in the attack chain by reducing the time needed to contain a threat, automating containment actions like isolating machines, blocking users, initiating scans, or triggering supplementary playbooks. Ultimately, automation empowers us to direct human efforts toward high-value activities like proactive threat hunting, curating threat intelligence for deployment in the Cyber Defense Center, and more, while enhancing the consistency, accuracy, and speed of addressing routine Security Operations tasks.

Log Management

All Azure resources have audit logging enabled for the Templafy Services. This includes SQL and storage accounts. All activity in the production environment performed by users and administrators are tracked. The SQL database logs are protected from modification and are kept for a minimum of 3 months. For Templafy Services, activity logs for administrator accounts are available in the admin portal of Templafy Hive. The following logs are available in our Admin Portal:

- User management activity logs: overview of all changes to users, such as invitation of new users and partners, changes to access privileges including removal, and all non-SSO sign-ins.
- Space members activity logs: overview of access assignments, changes and revocations for both individual users and groups, in relation to a specific space.
- Library admin activity logs: overview of all admin activity in the library, such as upload of templates or assets, renaming, editing (including tags and descripts), and deletion as well as changes to folders.
- Email signature activity logs: overview of all admin changes to email signatures from the admin center, such as creating, activating, deactivating or deleting a signature, changing its configuration, editing, and other changes to settings and content.

The Templafy status page can be used to see the status of Templafy, including individual components, including historical downtime.

For its internal infrastructure, Templafy collects, correlates, and analyzes data across accounts, devices, applications, and infrastructure using Azure Sentinel (SIEM) and the log data is retained for 6 months.

The information security team proactively hunts for threats reacts to threats that trigger pre-defined and configured alerts. Incidents are handled using the incident management process as described in the incident management section. All systems are configured with the same time and date to ensure traceability if an incident occurs.

Logical Security

A formal, documented user account and access provisioning process is in place to assign and revoke access rights to systems and applications. Access is allocated on a least privilege basis, which means by default, account access is denied until a business need is proven, and any additional privileges require approval. Templafy uses Azure AD for centralized authentication and authorization to restrict access to the systems and services within the Templafy environment. Each user account is unique and is identifiable to an individual user.

Periodic reviews of individual accounts and security group memberships are performed by assigned owners in coordination with the information security team, to evaluate and validate the user access. Remediation action is taken, as necessary, based on the review. Upon change of responsibilities, access rights are reviewed and addressed accordingly. Upon termination, access rights are revoked within 24 hours. User password standards are defined and implemented based on requirements outlined in the Templafy information security policies and the security best practices to enforce password quality, length, and complexity. Multi-factor authentication is enforced for critical systems, where supported.

Access to customer data through the Templafy solution by Templafy employees shall be granted only for customer support and success services offered in the best interest of the customer, or when a forensic investigation needs to be carried out following a security incident.

Customer tenant owners are responsible for reviewing access requests as well as updating the role of Templafy employees and partners within their tenant. Only customer owners and admins are able to enable automatic access for a list of authorized Templafy employees or Templafy partners. Once partner access has been enabled, customer owners will be able to decide if the access should be enabled indefinitely or for a set duration by specifying a revoke date. Access to program production data is restricted and limited to authorized personnel. Templafy has role-based access control to Kubernetes clusters. Access to production information systems is enforced via Azure AD multi-factor authentication. Appropriate identification and authentication are required to perform actions on the

production environment and cannot be circumvented. Read access to system databases is provided to Site Reliability Engineers. No one in Templafy has write access to production system databases.

Asset Management

Templafy has an asset management program that identifies information assets and defines appropriate protection responsibilities. Any assets associated with information and information processing facilities are identified and managed throughout their lifecycle in accordance with the information classification and handling procedures. The lifecycle of the information includes creation, processing, storage, transmission, deletion and destruction stages. All information assets have designated asset owners.

Information Classification And Handling

The information security team establishes and communicates an organization-wide information classification and handling policy and standard by which information is classified, defined, exemplified, and risk assessed. The standard clarifies to all Templafy employees how to handle information throughout the information lifecycle based on its classification. The lifecycle includes authorization, confidentiality, labeling, information transfer and storage protections, transportation, retention and disposal. The policy is reviewed annually or more frequently to address significant organization changes. All Templafy employees share the responsibility for ensuring that Templafy information receives an appropriate level of protection by observing the information classification restrictions and information handling process in the standard.

Data Loss Prevention

At Templafy we have implemented Data Loss Prevention (DLP) with a multifaceted approach in order to fortify the protection of sensitive information across its digital infrastructure. The cornerstone of this strategy lies in the formulation and strict enforcement of comprehensive labelling policies. These policies meticulously classify data based on its sensitivity level, attributing specific labels or metadata that distinctly identify the nature and confidentiality of each piece of information. These labels enable automated tracking and enforce controls to monitor, track, and safeguard the data as it traverses through different systems within our infrastructure. Templafy cultivates a culture of heightened awareness surrounding data protection. Through targeted awareness programs and continuous training initiatives, employees are educated about the criticality of safeguarding sensitive data and the implications of mishandling or unauthorized disclosure. These training courses not only outline the company's DLP policies but also emphasize the practical aspects of secure data handling, encompassing encryption methodologies, secure data sharing protocols, and the utilization of

authorized communication channels. Complementing these strategies, technical measures bolster the organization's DLP framework. Content inspection tools perform real-time scrutiny of data packets and files, employing contextual analysis to identify sensitive information patterns. Endpoint DLP solutions enforce data movement controls and encryption on devices, while network-based DLP monitors outgoing traffic and prevents unauthorized transfers. Encryption and tokenization secure data both in transit and at rest, while user activity monitoring tools track and detect anomalies in user behavior. Data masking techniques obscure sensitive information in non-production environments or reports. This combined approach not only strengthens the safeguarding of sensitive data but also significantly reduces the risks of data breaches and unauthorized disclosures.

Data Platform

Templafy's Data Platform is architected around the Data Lakehouse paradigm, leveraging Azure Synapse Analytics as its central component. This modern approach combines the flexibility of a data lake with the management features of a data warehouse. Our Data Team has implemented sophisticated internal tools that automate the deployment and integration of Azure services, ensuring a seamless, modular architecture.

For Business Intelligence (BI), we mainly utilize PowerBI, a robust tool that empowers us to create a range of internal dashboards. These dashboards play a crucial role in customer success, providing insights derived from aggregated data on user interactions with our product. This continuous analysis aids in the effective rollout of new features and strategic decision-making. It is important to note that these dashboards do not contain any Personally Identifiable Information (PII), ensuring compliance with privacy standards.

While PII is not present in our BI dashboards, it may be processed in certain data products for the purpose of analyzing customer usage patterns. This is essential for enhancing user experience and product development. To ensure utmost confidentiality and compliance, all PII data is segregated into a dedicated area within Azure. Access to this sensitive data is stringently controlled and limited to data engineers and analysts for specific, approved tasks.

Artificial Intelligence

Templafy leverages Artificial Intelligence in various aspects of the product. Tenant administrators and owners have the option to disable any of these AI functionalities in the Admin Center. All of Templafy's AI capabilities are built on standard Microsoft services.

Customer data is not used to train any of the AI models leveraged by Templafy's AI features. Only Templafy and Microsoft Azure are involved in the processing of data, with no additional third parties included.
Our main AI product is the AI Assistant which integrates seamlessly with the Office environment ensuring that end-users are encourages to adopt a protected iteration of AI using only centrally configured prompts. Any updates and patches to the AI Assistant are deployed in accordance with our Secure Software Development Lifecycle (see Software Development Lifecycle Section). The Azure Open AI models leveraged for the AI Assistant are stateless: no prompts or generations are stored in the model.
Templafy is committed to ensuring the responsible and ethical use of artificial intelligence within our organization. To support this commitment, we have implemented an Acceptable Use of AI included in our Acceptable Use Policy, which outlines clear guidelines for leveraging AI technologies in a manner that aligns with our values, compliance standards, and security requirements, as well as safeguarding intellectual property rights. Additionally, Templafy provides AI Awareness Trainings, ensuring employees understand the potential benefits and risks associated with AI.

Templafy Public API

The Templafy Public API serves as the interface for other applications to connect with Templafy. It facilitates the automation of administrative tasks that would typically require manual execution.

Templafy's Public API employs API keys for the authentication and authorization of users. These keys can be generated, managed, and revoked through the Templafy Admin Center. Only users with the necessary permissions are permitted to access the API, with actions limited by specific permissions and scopes, including library.read, library.readwrite, and datasources.readwrite.

To safeguard against misuse or abuse, Templafy implements rate limits on the public API. The system establishes two rate limits: a maximum of 500 calls every 10 seconds and 30,000 calls per hour. These restrictions are in place to maintain system performance and avert denial-of-service attacks.

Endpoint Management

All end-user laptops (Windows and MacOS) and mobile devices (iOS and Android) are centrally managed using mobile device management tool Microsoft Intune which enforce full disk encryption, endpoint protection, secure configuration and the ability to remote lock and remote wipe in the event a device is compromised. The Acceptable Use Policy requires that all work-related activities can only be done from devices that are managed by Templafy.

Templafy uses hardened baseline configurations deployed via Microsoft Intune. Full disk encryption is configured and enforced on all end-user laptops and desktops. Templafy continuously monitors all endpoints in conformity to Microsoft and industry best practices, CIS benchmarks, ISO/IEC 27001, ISO/IEC 27017 and SOC 2 compliance requirements and applies applicable recommendations and required remediations after review by the information security and IT teams. Anti-malware software with EDR capabilities is installed on all Windows and macOS workstations which is centrally managed and daily scanning is performed to detect any malware. Endpoints are configured with tamper protections to prevent impairment, disabling, or removal of anti-malware protection. Templafy has implemented a proactive strategy within our company by revoking local administrative rights for non-administrative users in order to create a more controlled and secure IT environment. This access limitation reduces the attack surface, in order to mitigate risks, enhance overall system integrity, and ensure the confidentiality of sensitive information.

Network Management

Azure Monitor is used to monitor the status and load of each managed network device. Azure Monitor provides detailed information of system metrics in dashboards and the ability to write custom queries to get essential data for all system behavior. It is used to monitor systems' current performance and investigate any irregularities from the past. The production environment has auto-scaling enabled. Templafy production data center network traffic is routed through a distributed denial-of-service (DDoS) protection service provided by Microsoft Azure to limit the effect of denial-of-service (DoS) attacks. The cloud guild in the engineering department holds routine meetings to review system capacity and environment health. All clusters have a georedundant failover location, to ensure continuous uptime and continuation of service.

All infrastructure and network changes are performed through Infrastructure-as-Code (IaC), and as such, is subject to the same rules as pull requests for code changes. This ensures the configuration is constantly checked against a set baseline.

The site reliability engineering team actively monitors network logging for the production network. Azure DDoS protection and Security Center generate alerts subject to review and investigation. An intrusion detection system (IDS) is configured to generate alerts following breaches of thresholds. Customer traffic is managed with load balancing.

All internal connections in the cluster are TLS 1.2 encrypted. All internal communication inside the Kubernetes cluster between microservices is running over HTTPS (by default traffic inside a Kubernetes cluster is not encrypted, as SSL traffic is terminated at the Ingress level). We added this extra layer of security, to ensure that even if one service is compromised, this cannot easily spread to other services.

All external network connections to the SQL server are protected by a firewall that verifies inbound traffic based on source and destination address, protocol and port. The site reliability engineering team maintains the whitelist regularly. Changes to the firewall are required to follow change procedures as described in the change management section.

Nginx is used as an ingress controller to route traffic to Kubernetes services. Nginx ingress controller is configured to force a redirect of all HTTP traffic on port 80 to HTTPS on port 443. Nginx is configured to use HTTP Strict Transport Security (HSTS). This means once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

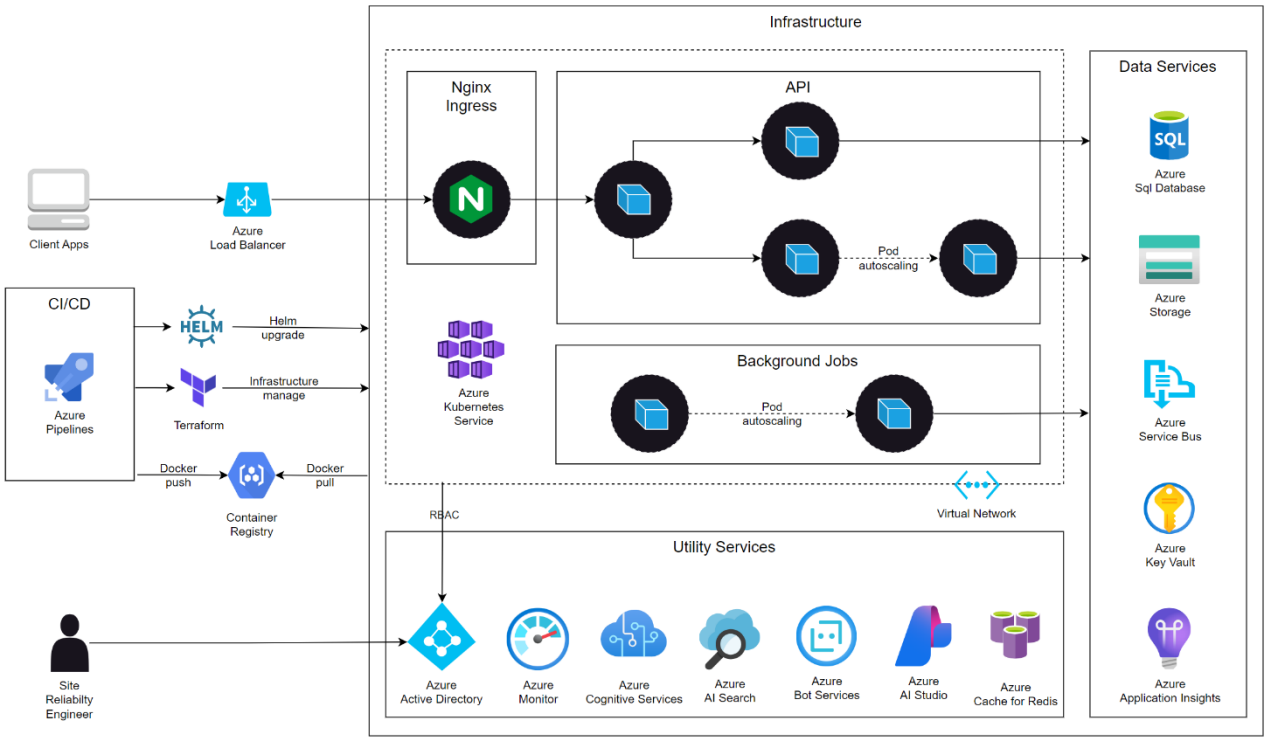

Figure 7 - Network Diagram

The corporate network supports internal business functions and is separate from the production network for each of the Templafy Services that support customer instances. Each corporate office location has multiple security controls to protect the network proportional to the risk assessment conducted on the network. Networking protocols that are not necessary for business purposes and/or are deemed to be non-secure are disabled. The corporate networks are segregated into VLANs based on business requirements.

Incident Management

Templafy has implemented an incident management policy that includes defined processes, roles, communications, responsibilities and procedures for detection, escalation and response to incidents internally and to customers.

Templafy's information security team uses the established incident classification, escalation and notification process for assessing an incident's criticality and severity. Response procedures are specific and reflect the nature of the incident. Incident and resolution analysis are carried out by the information security team to reduce the likelihood or impact of a future incident.

Incident procedures in relation to data privacy breaches have been implemented and include how and when to communicate with the data controller affected and the relevant authorities. Procedures for a forensic investigation of a security incident are in place when necessary to support potential legal action.

In the event of a Security Incident, Templafy provides customers with a detailed description of the Security Incident and the type of Personal Information concerned, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Templafy notifies without undue delay (and in any event within thirty-six (36) hours) inform affected customer in writing. Following the notification, Templafy takes reasonable steps to mitigate the effects of the Security Incident and to minimize any damage resulting from the Security Incident. Templafy assists and cooperates with affected customers with any necessary or appropriate disclosures and other investigative, remedial, and monitoring measures as a result of the security incident. Customers can report suspected security incident to Templafy via our external incident reporting form or through the email address security@templafy.com.

Incidents that impact availability of the Templafy Services are monitored and detected using Azure Application Insights and Container Insights. These alerts trigger PagerDuty which calls to action the site reliability engineers. The on-call responder identifies the incident severity. Depending on the severity, roles are assigned including primary responder, subject matter experts and communication coordinator. All activity around the incident is captured through video recording, internal notes and Azure DevOps Issue for tracking. A Blameless Postmortem is scheduled within six business hours of the resolved incident, inviting all the people involved in identifying, solving, and communicating about the incident. An official Postmortem, approved by Product Owners or CTO is posted to StatusPage for external communication in a timely manner.

Data Backup And Recovery

Data Backup: For Templafy Services, tenant configuration data and binary data are backed up daily in SQL. In Templafy Hive, a 90-day long-term backup retention geo-redundant backup of SQL is available. Templafy has GRS replication, soft delete for 30 days for blob storages and containers. Assets are stored in immutable blob storage where the data cannot be deleted neither intentionally nor unintentionally. Data in storage accounts are written to three disks for redundancy per site and replicated across multiple sites. The backup system automatically generates a backup log. A point-in-time restoration option is also enabled for up to 7 days, in which all changes can be restored with at most 10 minutes of data lost. Access to backup data is restricted only to authorized personnel using Azure AD with multifactor authentication. Furthermore, all backups are encrypted using AES 256 encryption.

Redundancy: Templafy uses multi-site data centers with availability commitments to permit the resumption of Templafy Services in the event of a disaster or partial outage at its primary data center location. Templafy has a documented disaster recovery plan. This plan is reviewed and tested at least annually, and test results are reviewed by plan stakeholders. When necessary, plan documentation is updated.

Business continuity and disaster recovery: Templafy prioritizes the availability of the Templafy Services to its customers and plans for a variety of situations that may impact them. Templafy has established an organization-wide Business Continuity Policy that serves as a guideline for implementing uniform business continuity plans. Risk assessments are conducted to identify and assess business continuity risks across all office locations and Azure services. Protection measures are put into place to react to natural and human-made threats accordingly. Templafy has created Disaster Recovery plans to cover all three general scenarios: malicious incidents (third-party or insider threat), accidental incidents (human error) and unavailability incidents (Azure outages that affects our product). Templafy conducts testing of the business continuity and disaster recovery plans annually. Any issues identified during testing are resolved, and plans are updated accordingly. The business continuity plans are reviewed annually and updated, if necessary. Testing of plans include failing over a server and restoring of backups. The business continuity plans cover the key personnel, resources and actions required to continue critical business processes and operations. Templafy performs an annual Business Impact Analysis (BIA) to identify the operational and financial impacts of any unplanned disruption to Templafy's business operations. The results of the BIA are integrated into the business continuity plans when relevant.

Physical Security

Data center security: No servers or computer facilities for the Templafy Services are hosted onsite. All physical access to facilities and environmental controls are controlled at the Cloud Service Provider (CSP) locations of Microsoft. Stringent physical and operational controls are in place and are accounted for by Microsoft's numerous ISO certifications and standard compliance, which are reviewed during the sub-processor annual evaluation by the information security team against Templafy's information security requirements, as described in the supplier management section.

Office security: Templafy maintains a physical and environment policy for its offices to ensure the security and integrity of Templafy's facilities and the assets located within. Templafy has physically sound buildings protected by appropriate security controls such as alarms, locks, reinforced windows, and emergency equipment. Keycard controlled locked access is in use and are timely removed as described in the logical security section. Visitors to secure areas are required to sign in and out with arrival and departure times, are required to wear an identification badge, and always escorted while in secure areas. Delivery and loading areas are managed and appropriately protected.

Supplier management

Templafy has established an organization-wide Supplier Risk Management policy and standard to manage supplier relationships with a risk-based approach in line with the information security objective. It covers key supplier lifecycle stages supplier onboarding, monitoring and offboarding. The policy outlines the controls that are implemented to ensure that suppliers live up to security and privacy requirements laid out by Templafy, and that this is appropriately managed by Templafy personnel involved in supplier relationships. The policy applies to all suppliers used by Templafy that have access to or process Templafy information, and thus must adhere to Templafy's information security requirements. This includes Templafy's sub-processors.

Supplier assessments and monitoring: All suppliers undergo a procurement assessment to identify the amount and severity of risks involved in the supplier relationship, as well as how critical the relationship is to the business at the procurement phase and are monitored thereafter at a frequency proportional to the calculated level of criticality and level of risk. Supplier reviews are also carried out ad-hoc upon relevant changes in the scope of the service provided by the supplier. More thorough assessments on security and privacy are conducted to ensure that suppliers meet the minimum information security requirements set out by Templafy. Depending on the supplier, assessments may be in the form of one or more of the following:

- Questionnaires filled out by the supplier, Templafy, or both. These may be following standard security framework e.g., ISO27001) and/or standard security questionnaires e.g., SIG, or custom-made by Templafy.
- Review of audit reports and/or certificates, e.g., ISO27001, SOC 2.
- Technical review meetings with the potential supplier.
- Reviewing further evidence such as suppliers' written policies or SOPs.
- Other means deemed applicable to the nature of the supplier relationship in question.

Suppliers are offboarded in a systematic and thorough manner, ensuring that all logical and physical access to company resources is completely removed. This process involves revoking permissions to systems, applications, and networks that the suppliers might have previously had access to. Templafy ensures that any contractual agreements regarding data handling, storage, and deletion are adhered to upon contract termination.

Supplier agreements: Templafy enters appropriate contractual agreements with suppliers. Depending on the supplier relationship, multiple agreements may be required, e.g., information security requirements, data privacy requirements, service level agreements, data processing agreements. All sub-processors have data processing agreements and are updated on a frequent basis subject to regulation changes. Templafy requires that suppliers sign a confidentiality and non-disclosure agreement prior to sharing confidential information.

Privacy

Templafy has a dedicated Privacy team with responsibility for compliance with legal and contractual requirements in relation to the customer end-users' right to privacy. The data processing agreement (DPA) with customers governs the processing that Templafy undertakes as a data processor on behalf of customers, including provisions about purpose limitation, international data transfers, sub-processors, data subject requests and data breach notifications. Processing of personal data for other purposes than the services are subject to strict data controller obligations under the GDPR, and are made transparent in the Templafy privacy policies.

The Privacy team is involved in any and all suspected and actual information security incidents that involve personal data, including pseudonymized data, to ensure the breach response is compliant with privacy law requirements, such as notification to customers, data subjects and/or the authorities, as appropriate.

Sub-processors are classified as critical suppliers, thus subject to the strictest requirements under the supplier management process described in the Supplier assessments and monitoring section. They are contractually bound to at least the same level of data protection as stipulated in the customer DPAs.

Sub-processing activities only occur upon legal bases for transfer, e.g. the Data Privacy Framework (DPF) program, Standard Contractual Clauses (SCCs) and/or Transfer Impact Assessments (TIA) as appropriate. Templafy is certified under the DPF program and is registered with the UK ICO (Information Commissioner's Office).

Internally, Templafy prioritizes the protection of personal data and ensures compliance with privacy regulations across all our operations. We conduct Data Protection Impact Assessments (DPIAs) on our core processes as part of our commitment to identifying and mitigating risks associated with data processing activities. This proactive approach helps us safeguard privacy and uphold transparency in how data is handled. Additionally, we have implemented a comprehensive Employee Privacy Policy, which outlines the measures we take to protect the personal data of our workforce. This policy ensures employees are informed about their privacy rights and the steps we take to maintain confidentiality and trust.

Information And Communication

Internal Communication: Templafy communicates the information security program in various ways via security awareness training, town hall meetings, internal communications via email and messaging tools, policies and procedures uploaded to the Templafy's internal SharePoint site and verbally through daily interaction with the information security team.

External Communication:

Customers can request meetings with security personnel during procurement and at any stage during customer use of Templafy Services. Upon request, customers can receive security documentation, including the latest penetration testing results, latest external audit reports such as ISO27001 and SOC 2. Customers can report security incidents directly to security@templafy.com. Customers may view the most recent general terms and conditions, service level agreements and data processing agreements on the Templafy website. Communication with customers and partners can include their review of blog posts and knowledge base articles, as well as communication related to the resolution of submitted support cases on Templafy's ticketing system through the Templafy website.

Monitoring

Internal Audit: Templafy has an internal audit function independent from control design and implementation periodically audits each area of Templafy's ISMS.

Legislative And Contractual Compliance

Contractual and legislative requirements are registered, reviewed, updated, and compliance monitored on an ongoing basis.

Knowledge And Research

The Information Security team is responsible for keeping updated with changes in the cybersecurity and data protection threat landscape, through periodic research and contact with special interest groups, specialist security forums and professional associations.

Changes To The System During The Period

There were no changes that are likely to affect report users' understanding of how Templafy provides the Templafy Services during the period January 1st, 2024 to December 31st, 2024.

Disclosure Of Incidents

There were no system incidents during the period January 1st, 2024 to December 31st, 2024 requiring disclosure that either where the result of controls failing; or, resulted in a significant impairment to the achievement of systems requirements or service commitments to customers.

Complementary User Entity Controls

Templafy Services are designed with the assumption that certain controls will be implemented by user entities.

#	Complementary user entity control
1	User entities are responsible for understanding and complying with their contractual obligations to Templafy.
2	User entities are responsible for monitoring and enforcing organizational compliance with Templafy's terms and agreements.
3	User entities are responsible for keeping the primary, service, security, billing and administrative contact information on file with Templafy updated.
4	User entities are responsible for immediately notifying Templafy of any actual or suspected information security breaches, including compromised user accounts, to security@templafy.com.
5	User entities are responsible for deploying releases of the Templafy Desktop MSI package without undue delay
6	User entities are responsible for providing accurate and complete information and documentation regarding their own authentication method for authentication setup.
7	User entities are responsible for protecting established user IDs, passwords, and other credentials within their organizations, including appropriate safeguards for devices running Templafy applications.
8	User entities are responsible for maintaining their own signing certificate for SSO authentication methods and ensuring Templafy's technical operation teams receive updated certificate no later than three weeks before expiration.
9	User entities are responsible for reviewing their own access to Templafy periodically to validate the appropriateness of access levels, including any third-party access they may have granted.
10	User entities are responsible for removing terminated or unwanted user accounts from the system either manually with the use of the deletion feature made available by Templafy or through SCIM in a timely manner.

11	User entities are responsible for ensuring the appropriateness of designated administrators and maintaining a low administrator count according to the principle of least privilege.
12	User entities are responsible for informing Templafy of changes to their infrastructure (e.g., network ports and proxy settings) or application environment (Office platform, OS platform, Desktop/Application Virtualization) in order to ensure the continued functioning and support of Templafy.

Figure 8 - User Entity Responsibility

Complementary Subservice Organization Controls

Templafy uses subservice organizations for data center hosting and infrastructure services in support of its document creation, collaboration and email signature system. Templafy runs on Microsoft Azure Platform-as-a-Service, which provides many enhanced features for security, availability and scalability out of the box. There are clear lines of responsibility, but often, there are also shared roles when it comes to responsibility regarding security in the cloud. Templafy conducts due diligence towards Microsoft Azure annually to monitor the outsourced operations. This is achieved by reviewing Microsoft's SOC 2 and other compliance reports, as well as having the necessary agreements in place.

Control Activity Expected To Be Implemented By Subservice Organization	Subservice Organization	Applicable Trust Services
Physical access to the data center facility is restricted to authorized personnel.	Microsoft Azure	CC6.4, CC6.5
Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) are implemented to safeguard sensitive data and information systems.	Microsoft Azure	CC6.2, CC6.3, CC6.4, CC6.5
The data center facility is monitored 24x7 by security personnel	Microsoft Azure	CC6.4, CC7.2
All production media is securely decommissioned and physically destroyed prior to leaving the data center.	Microsoft Azure	CC6.5

External vulnerability assessments are performed on a periodic basis, identified issues are investigated and tracked to resolution in a timely manner.	Microsoft Azure	CC7.1
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically	Microsoft Azure	A.1.3
Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.	Microsoft Azure	CC6.1, CC6.2, CC6.3, CC6.5, CC7.2

Figure 9 - Subservice Organization Controls