Chapter 1: Introduction

Purpose

This Security Policy is established to protect user data, ensure system integrity, and prevent unauthorized access, thereby enhancing user confidence in our services. It serves to demonstrate our commitment to security and outlines the measures we implement to safeguard digital and physical assets against potential threats. Prioritizing data privacy and network security, this document details our protocols designed to uphold these standards.

Scope

This policy applies universally to all our operations involving digital project uploads and rendering services at our datacenters. It encompasses all datacenter operations and physical infrastructures where user data is handled, processed, or stored. The guidelines within this policy cover every aspect of security from data entry to final data deletion and are designed to ensure comprehensive protection across all platforms and interactions.

Responsibility

- **Global Security Team:** This team is tasked with monitoring for security breaches and potential threats. Their role is crucial in maintaining our high standards of security by providing timely warnings and actions against any detected vulnerabilities.
- **IT Staff:** Our IT personnel are rigorously trained and are key enforcers of this security policy. They are responsible for implementing and maintaining our security infrastructure and responding to security incidents.
- **Data Handling Staff:** A select group of trained employees has access to user data. These individuals are well-versed in our security protocols and adhere strictly to this policy to ensure the highest levels of data privacy and integrity.

Oversight and Compliance

- **Security Oversight:** Multiple internal and external parties are involved in overseeing our security operations. This includes the Head of Security at our datacenter and security staff stationed at physical locations.
- **External Partners:** The Digital Trust Center, a governmental body, collaborates with Previder and other external agencies to oversee and ensure compliance with established security standards. Their involvement provides an additional layer of assurance and oversight, contributing to robust security governance.

Chapter 2: User Access Control

Authentication Methods

Physical Access

Access to the datacenter is restricted to authorized personnel using a multi-factor authentication process involving a digital key, biometric (fingerprint) scanning, and a PIN for machine rack access. This stringent process ensures that only authorized staff can enter and interact with critical infrastructure.

Network Access

Remote access to machines is safeguarded through a security password and an additional password on the master machine, ensuring that only designated personnel can control these systems remotely.

Compliance and Security Checks

All security systems are routinely checked and certified by the Dutch Data Center Association to meet the highest security standards, with regular audits conducted monthly.

Authorization Levels

Access Privileges

Access levels within the company are strictly defined based on the employee's role, ensuring individuals have only the necessary privileges to perform their duties. This is controlled through password protection and logical access controls to sensitive data and servers.

Account Management

- Only two high-level employees have the authority to create or delete accounts, providing tight control over access credentials.
- An internal review and approval process is mandatory for all new account setups or modifications to existing accounts.

Access Review and Revocation

- User access rights are reviewed annually in conjunction with employee performance evaluations to ensure access levels remain appropriate.
- Access is promptly revoked when no longer needed, or if a security risk is identified, to maintain a secure IT environment.

Remote Access

- Specific team members have remote access capabilities; developers can access the website's database hosted on Amazon AWS, and support staff can access the master computer in the datacenter.
- All remote access is secured with two-factor authentication (2FA), providing an additional layer of security.

Monitoring and Logging

- Changes to the website and database are tracked using Git, allowing comprehensive oversight of modifications by the Head Developer.
- Remote access sessions to the master computer are logged through our remote access software, with logs maintained for three months to aid in audits and security reviews.

Chapter 3: Data Security

Data Encryption

- All user projects and associated data are encrypted using OpenSSL with AES-256 encryption and 2048-bit RSA data encryption standards. This applies to data both in transit and at rest, providing a robust shield against unauthorized access.

- Uniform encryption practices are maintained across all stages of data handling, ensuring consistent security from upload to storage.

Data Retention and Deletion

Retention Policy

- All data, including 3D project files and rendered outputs, is retained on our systems for a maximum of 7 days to facilitate user access and efficiency in re-uploads and downloads. This is managed through our synchronized system architecture.
- Automated backend processes are configured to delete all data post the 7-day retention period, ensuring compliance with our data governance policies.

Secure Deletion Practices

- Data deletion is carried out using reliable mechanisms within our central NAS configured in RAID 10 setup, which also minimizes the risk of data loss due to hardware failures. Once deleted from the NAS, the data is irrecoverably removed, maintaining data privacy and security.

Backup and Recovery

Backup Protocols

- Daily backups of the entire backend system are performed, which include all active render jobs, user data, credits, and system settings. These backups are stored on a separate network disk and also synced with Amazon Cloud for additional security.
- The website and its database are similarly backed up daily on Amazon Cloud. Notably, individual project files and user outputs are not included in these backups to prevent excessive data storage and maintain user data confidentiality.

Disaster Recovery

- Our comprehensive backup strategy enables swift recovery from various scenarios, including hardware malfunctions and data corruption.
- Regular testing of the disaster recovery plan occurs monthly, ensuring its effectiveness and our ability to promptly restore operations without significant data loss.

Chapter 4: Network Security

Firewalls and Intrusion Detection Systems

Firewall Implementation

- Multiple layers of firewall protection are deployed across our network, including hardware-based firewalls on all machines and additional software firewalls within our systems. This robust configuration ensures that only authorized files and data can enter our network.
- Our systems are specifically configured to only accept file types that are part of a 3D project, significantly reducing the risk of malicious file uploads.

Intrusion Detection Systems (IDS)

- We utilize a proprietary IDS that scrutinizes all incoming files for compliance with our security standards. Any file with extensions that are not pre-approved is automatically removed to prevent potential security breaches.
- This system is capable of identifying and eliminating scripts and executables that could be harmful, with all operations managed and regularly updated by our skilled backend developers.

Secure File Transfer

Protocols and Encryption

- Secure file transfers are facilitated using HTTPS and FTPS, incorporating OpenSSL with AES-256 encryption and 2048-bit RSA data encryption to safeguard data in transit.
- This stringent encryption setup ensures that all data, whether incoming or outgoing, is robustly encrypted using contemporary security protocols.

Network Monitoring

Monitoring Tools

- Our network is constantly monitored by an advanced backend system that not only tracks all data transfers but also assesses the security of files both pre- and post-upload. This system is designed to detect and respond to any signs of unauthorized access or potential security threats.

Operational Procedures

- Upon detection of any anomaly or suspicious activity, our system automatically initiates security protocols to isolate and mitigate potential threats. This proactive approach allows us to maintain high security standards and react quickly to potential issues.

Response to Anomalies

- If a potential security threat is detected, the issue is immediately escalated to our security team. The team follows a structured incident response protocol which includes assessment, containment, eradication, and recovery phases to effectively manage and resolve the situation.
- Responsibility for overseeing this process lies with our security team leaders, who coordinate response efforts and ensure that all security breaches are handled swiftly and efficiently.

Chapter 5: Physical Security

Datacenter Security

Physical Access Controls

- Access to the datacenter is controlled through a multi-factor authentication system that includes a digital key, biometric (fingerprint) scanning, and a PIN for specific areas like machine racks. This stringent process is designed to ensure that only authorized personnel can access sensitive areas, effectively safeguarding critical infrastructure against unauthorized entry.

System Integrity and Tamper-Proofing

- All access control systems are regularly tested and updated to maintain their operational integrity and to prevent tampering. Regular audits and checks are performed to ensure that these systems meet the latest security standards and are resistant to physical and digital tampering efforts.

Security Personnel

Roles and Responsibilities

- Security personnel at the datacenter are responsible for monitoring physical access, conducting regular security patrols, and responding to security alerts. Their duties also include maintaining the security of the physical site and managing emergency situations as they arise.

Contractual Employment

- The security staff are contracted through Previder, our datacenter partner, ensuring that all personnel are highly trained and meet our stringent security requirements. This arrangement allows for specialized security expertise and flexible staffing solutions.

Environmental Controls

Safety and Protection Systems

- Our facilities are equipped with state-of-the-art HVAC systems and advanced fire suppression technologies to protect against environmental hazards. These systems are critical for maintaining optimal conditions within the datacenter and for protecting hardware from damage due to temperature fluctuations or fire.

Maintenance and Testing

- These environmental control systems are subjected to rigorous maintenance and testing schedules to ensure they are always functional. Regular checks and updates are conducted by certified technicians to uphold safety standards and to prevent any failures during critical operations.

Hardware Security

Securing Sensitive Equipment

- Sensitive hardware such as servers and storage devices are housed in secured enclosures with restricted access. These enclosures are equipped with locking mechanisms that require authorization for access, minimizing the risk of physical tampering.

Dedicated Security Zones

- Critical hardware areas are designated as high-security zones within the datacenter. Access to these zones is limited to a small number of authorized personnel, and monitored by CCTV systems to ensure that unauthorized access or tampering does not occur.

Surveillance and Monitoring

Surveillance Systems

- Comprehensive CCTV systems and motion detectors are installed throughout the datacenter and other critical locations to monitor for any unusual activity. These surveillance tools play a key role in our security strategy by providing real-time monitoring of physical movements.

Data Management and Privacy

- Surveillance footage is carefully monitored and stored in secure locations with restricted access. Data privacy protocols are strictly followed to ensure that all surveillance data is handled responsibly and ethically, with footage being used solely for security purposes.

Chapter 6: Incident Response

Incident Detection and Analysis

Detection Tools

- Our security infrastructure includes advanced firewall technologies and proprietary backend software designed to detect unusual activities and potential security threats. These tools are integral to our proactive monitoring strategy.

Operational Protocols

- The tools are configured to analyze network traffic and system activity for anomalies that could indicate a security incident. Automated alerts are generated based on predefined criteria such as unusual access patterns or unauthorized attempts to access sensitive data.

Roles and Responsibilities

- The Head of Security oversees the monitoring of detection tools and is responsible for the initial assessment of alerts. Upon detecting a potential incident, they are tasked with escalating the situation according to the severity and potential impact on our operations.

Response Strategy

Immediate Actions

- Upon identification of a security incident, immediate actions include isolating affected systems to prevent further damage and assessing the scope and impact of the breach. These initial steps are

crucial for containing the incident and mitigating any adverse effects.

Incident Classification

- Incidents are classified according to their severity, which helps in prioritizing our response efforts and allocating resources effectively. This classification is based on the potential impact on our business and the sensitivity of compromised data.

Communication Procedures

- Key personnel within IT and senior management are promptly notified about the incident through encrypted communication channels to ensure confidentiality and swift action.
- External communications, if necessary, are handled by a designated spokesperson to ensure consistent and accurate messaging to stakeholders and the public.

Recovery and Post-Incident Analysis

Recovery Operations

- System recovery is initiated immediately, with predefined procedures to restore operations within 30 minutes for software-related issues, thanks to our robust backup systems. Hardware issues are addressed by replacing affected components with ready-to-deploy spares.
- Recovery time objectives (RTOs) are set at 30 minutes during working hours, ensuring minimal disruption to our services.

Post-Incident Review

- Following a security incident, a thorough analysis is conducted to determine the root cause and evaluate the response efficacy. This review involves key members from our security and IT teams.
- Lessons learned from the incident are integrated into our ongoing security strategy to enhance our resilience and response capabilities for future incidents. Adjustments may include updates to our security protocols, training for personnel, and improvements in our monitoring and detection systems.

Chapter 7: Compliance and Auditing

Requlatory Compliance

Adherence to Legal Standards

- Our operations are fully compliant with the General Data Protection Regulation (GDPR), ensuring the highest standards of privacy and data protection for our users. We conduct regular reviews of our compliance measures to keep up with any changes in the law.

Compliance Measures

- To guarantee compliance, we implement strict data handling and processing protocols, which are regularly reviewed and updated. These include securing user consent for data processing, ensuring data minimization, and maintaining transparency about data use.

Data Protection Oversight

- The role of overseeing data protection standards and compliance is integrated within the responsibilities of our Head of Security. This ensures that our data protection efforts are aligned with our broader security policies.

Security Audits

Audit Frequency and Scope

- Security audits are conducted quarterly to ensure that all aspects of our security infrastructure meet or exceed industry standards. These audits are a mix of internal reviews conducted by our own audit team and external evaluations handled by independent auditors.
- Audits comprehensively cover network and data security, physical security measures, and compliance with privacy laws.

Audit Execution

- Our audit procedures involve systematic checks of all security systems and controls. This includes reviewing access logs, testing security protocols, inspecting physical security measures, and assessing compliance with data protection regulations. The thoroughness of these audits helps in identifying and mitigating any potential security vulnerabilities.

Penetration Testing

Testing Frequency and Areas

- Penetration testing is performed monthly to proactively identify and address vulnerabilities. These tests primarily focus on evaluating the security of our web applications and network infrastructure.

Vulnerability Management

- Findings from penetration tests are immediately escalated to our security team, who prioritize the remediation based on the severity of the vulnerability. This rapid response ensures that potential security issues are addressed promptly and effectively.
- A detailed action plan is developed for each identified issue, and progress on remediation efforts is closely monitored by the Head of Security. This systematic approach helps in strengthening our defenses and reducing the risk of security breaches.

Chapter 8: User Education and Awareness

Training Programs

Training Content and Frequency

- Our security training programs are comprehensive and mandatory for all employees, covering topics such as data protection, incident response procedures, and safe internet practices. These training sessions are held annually to ensure that all team members are updated on the latest security protocols and threats.

Training Formats

- Given our team's size and structure, training is typically delivered in the form of in-person meetings and presentations. This format allows for interactive discussions and immediate feedback on complex topics, facilitating a deeper understanding of the material presented.

Security Updates

Information Dissemination

- Security information is primarily communicated through personal communications or during scheduled meetings where security updates and policies are a standing agenda item. This

approach ensures that all team members are informed and can discuss new threats or changes in policies in real-time.

Regular Updates

- During these meetings, we also discuss recent security threats and any relevant updates to our security strategies. This regular review helps maintain a high level of awareness and preparedness among our staff.

Engagement Strategies

Maintaining Engagement

- Our approach to engaging staff in security matters is integrated into their professional development. By recruiting highly trained professionals and fostering a culture of continuous improvement, we ensure that security remains a priority for all employees without the need for additional enforcement or engagement strategies.

Chapter 9: Software and Application Security

Development Security

Security Practices in Development

- Our development team adheres to best practice security protocols throughout the software creation process. This includes secure coding practices to prevent common vulnerabilities and regular code reviews to ensure quality and security.

Integration of Security in SDLC

- Security is a foundational aspect of our software development lifecycle. Although formal security audits are reserved for major changes, ongoing informal reviews and discussions about security occur at all stages of development, involving all relevant personnel.

Patch Management

Patch Management Procedures

- Patch management is a critical function performed by our IT staff, focusing on keeping all network components, datacenter hardware, and software applications up to date. Patches for our proprietary software are developed continuously as vulnerabilities are identified, ensuring rapid deployment and minimal risk.
- Our approach ensures that all systems, including operating systems like Windows, are updated at regular intervals (every two months for OS patches) and more frequently as needed for critical vulnerabilities.

Response to Vulnerabilities

Vulnerability Management

- When vulnerabilities are discovered, they are promptly addressed by our development team. A structured process is in place to develop, test, and deploy patches efficiently to mitigate any potential security risks.

Application Security

Proactive Security Measures

- To protect our applications from external threats, we implement several security measures, including the use of Web Application Firewalls and rigorous security testing routines.
- Applications are continuously monitored for signs of security breaches, and potential threats are addressed immediately to prevent any exploitation.

Security Testing

Testing Protocols

- Our security strategy includes comprehensive testing such as penetration testing and vulnerability scanning to identify and address potential security issues before they can be exploited.
- These tests are conducted regularly, ensuring that our applications remain secure against evolving threats.

Chapter 10: Third-Party Security

Overview of Third-Party Interactions

Limited Third-Party Access

- Our operations rely minimally on third-party vendors, with the only external collaboration being with our datacenter partner, Previder. This partner manages network-related tasks and does not have access to our core systems or data, thereby significantly reducing potential security risks.

Vendor Management

Vendor Selection and Security Assessments

- Given our current operational model, we do not engage with third-party vendors who require access to our system or sensitive data. As such, there are no ongoing vendor selection processes or security assessments specifically related to these types of third parties.

Contractual Obligations and Compliance

Security Clauses and Monitoring

- For necessary external services, such as those provided by our datacenter, stringent security clauses are included in all contracts to ensure the highest standards of security are maintained. Compliance with these clauses is closely monitored through regular reviews and audits conducted by our internal security team.

Supply Chain Security (Not Applicable)

Risk Management and Collaboration

- Our current business model does not involve a complex supply chain with multiple vendors, thus minimizing the security risks associated with such arrangements. Any potential future changes to this model will be accompanied by comprehensive risk assessments and the implementation of appropriate security measures.

Future Considerations

Planning for Potential Third-Party Engagements

- Should our business strategy evolve to include more significant interactions with third-party vendors or an expanded supply chain, we will develop and implement rigorous security protocols.

This will include vendor security assessments, enhanced contractual obligations, and dedicated monitoring practices to safeguard our operations.

Chapter 11: Policy Review and Update

Policy Review Process

Review Frequency and Triggers

- Our security policy is formally reviewed annually to ensure it continues to meet the evolving security needs of our organization. Additionally, reviews may be triggered by significant events such as security breaches or major technological changes that could impact our security posture.

Review Committee

- The review process is overseen by a dedicated committee consisting of the CEO and the Head of Security. This committee is responsible for evaluating the relevance and effectiveness of the policy and making recommendations for improvements.
- Their roles include gathering input from various department heads, assessing current security threats, and aligning the security policy with organizational goals and compliance requirements.

Policy Updates

Updating Procedures

- Updates to the security policy are managed through a structured process that includes drafting changes, reviewing them for potential impacts, and obtaining approval from key executives before implementation.
- Once updates are approved, they are systematically implemented across the organization to ensure all systems and processes are in compliance with the new policy standards.

Documentation and Communication

- Changes to the policy are meticulously documented and stored in a central online repository accessible to all employees. This ensures that everyone has access to the latest version of the policy.

- Updated policies are communicated through detailed presentations during scheduled meetings, allowing for direct discussion and clarification of new procedures and standards.

Continuous Improvement

Feedback Mechanisms

- Feedback on the security policy is actively encouraged and primarily collected during regular team meetings. This feedback is crucial for continuous improvement and helps identify areas where the policy may need refinement.
- A formal feedback loop is integrated into our policy review process, where suggestions and concerns raised by employees are systematically evaluated and addressed by the review committee.