Security Whitepaper

Craic Studio LLC

SOC 2 Readiness & Security Policies

Information Security Policy

Information Security Policy

#1. Overview

##1.1 Purpose
The purpose of this Information Security Policy (ISP) is to establish the high-level directive and strategic approach of Craic Studio LLC ("the Company") regarding the protection of its information assets. This policy serves as the foundation for the Company's Information Security Management System (ISMS) and demonstrates our unwavering commitment to protecting the confidentiality, integrity, and availability of data entrusted to us by our clients, employees, and partners.

##1.2 Scope
This policy applies to all employees, contractors, consultants, temporary staff, and third-party vendors (''Personnel'') who have access to Craic Studio LLC's systems, networks, data, or physical facilities. It covers all information assets, including but not limited to customer data, proprietary software code, intellectual property, financial information, and employee records, regardless of the format (electronic or physical) or location (on-premise or cloud-based).

#2. Policy Statement

##2.1 Management Commitment
Craic Studio LLC's leadership is committed to:
- Allocating appropriate resources to the information security program.
- Ensuring that security activities are aligned with business objectives.
- Communicating the importance of effective information security management to all personnel.
- Promoting continual improvement of the ISMS.

##2.2 Security Objectives
Our primary security objectives are to:
- **Confidentiality:** Ensure that information is accessible only to those authorized to have access.
- **Integrity:** Safeguard the accuracy and completeness of information and processing methods.
- **Availability:** Ensure that authorized users have access to information and associated assets when required.
- **Compliance:** Adhere to applicable legal, regulatory, and contractual requirements, specifically aligning with the AICPA SOC 2 Trust Service Criteria.

#3. Roles and Responsibilities

##3.1 Security Officer
The Owner/Lead Developer serves as the designated Security Officer and is responsible for:
- Developing, implementing, and maintaining the information security program.
- Conducting regular risk assessments.
- Reviewing and approving security policies and procedures.
- Coordinating incident response activities.

##3.2 Personnel
All personnel are responsible for:

- Reading, understanding, and complying with this policy and all supporting procedures.
- Reporting any actual or suspected security incidents or weaknesses immediately.
- Protecting their authentication credentials (passwords, tokens, etc.).

#4. Risk Management

##4.1 Risk Assessment
The Company shall conduct a formal risk assessment at least annually or upon significant changes to the business, technical, or threat environment. This process involves identifying assets, threats, and vulnerabilities, and evaluating the likelihood and impact of potential security events.

##4.2 Risk Treatment
Based on the results of the risk assessment, the Company will implement appropriate controls to mitigate risks to an acceptable level. Residual risks must be formally accepted by management.

#5. Compliance and Enforcement

##5.1 Compliance
Compliance with this policy is mandatory. The Security Officer will verify compliance through periodic audits, monitoring, and reporting.

##5.2 Exceptions
Any exceptions to this policy must be documented and approved in writing by the Security Officer. Exceptions will be reviewed periodically to determine if they are still necessary.

##5.3 Enforcement
Violation of this policy may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.

#6. Policy Review
This policy will be reviewed at least annually to ensure its continued suitability, adequacy, and effectiveness. Updates will be communicated to all relevant personnel.

Acceptable Use Policy

Acceptable Use Policy

#1. Overview

##1.1 Purpose
The Acceptable Use Policy (AUP) defines the standards for the acceptable use of Craic Studio LLC's computing resources. The goal is to ensure that these resources are used for appropriate business purposes and to protect the Company from legal liability, reputational damage, and security risks.

##1.2 Scope
This policy applies to all users of Craic Studio LLC's information technology resources, including but not limited to computer systems, mobile devices, software, internet access, email, and cloud services (e.g., Supabase, Vercel, GitHub).

#2. General Use and Ownership

##2.1 Ownership
All data created, stored, processed, or transmitted on Company systems is the property of Craic Studio LLC. Users should have no expectation of privacy regarding any activity performed on Company-owned or managed systems.

##2.2 Monitoring
The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. This may include monitoring email, internet usage, and file transfers.

#3. Acceptable Use Guidelines

##3.1 Business Use
Company resources are provided primarily for business purposes. Incidental personal use is permitted provided that it:
- Does not interfere with the user's productivity or work duties.
- Does not violate any applicable laws or Company policies.
- Does not consume excessive system resources.

##3.2 Professional Conduct
Users must communicate in a professional manner. The transmission of material that is harassing, discriminatory, defamatory, fraudulent, or otherwise offensive is strictly prohibited.

#4. Prohibited Activities

##4.1 System and Network Activities
The following activities are strictly prohibited:
- Attempting to circumvent user authentication or security of any host, network, or account.
- Unauthorized scanning or probing of networks (port scanning, vulnerability scanning) without explicit authorization.
- Interfering with or denying service to any user (e.g., denial of service attacks).
- Installing unauthorized software or hardware on Company systems.

##4.2 Data Security
- Users must not transfer Company data to unauthorized personal devices or cloud storage services.
- Users must not share their passwords, API keys, or MFA tokens with anyone, including other employees.
- Users must not access data for which they do not have a legitimate business need.

##4.3 Copyright and Licensing
- Users must not download, install, or distribute software, media, or other materials in violation of copyright laws or license agreements.

#5. Mobile and Remote Work

##5.1 Device Security
- All devices used to access Company data must be secured with a strong password or biometric lock.
- Full-disk encryption must be enabled on all laptops and mobile devices.
- Devices must be kept up-to-date with the latest operating system security patches.

##5.2 Public Wi-Fi
- Users must avoid using unsecured public Wi-Fi networks to access Company data. If necessary, a VPN must be used to encrypt traffic.

#6. Reporting Violations
Users are required to report any known or suspected violations of this policy to the Security Officer immediately. Failure to report a violation may itself be considered a violation of this policy.

Access Control Policy

Access Control Policy

#1. Overview

##1.1 Purpose
This policy establishes the framework for managing access to Craic Studio LLC's information systems and data. It ensures that access is granted in a controlled manner, based on business requirements, and effectively managed throughout the user lifecycle.

##1.2 Scope
This policy applies to all logical access to Company systems, applications, databases, and network infrastructure.

#2. Access Control Principles

##2.1 Principle of Least Privilege
Access rights are granted based on the "Principle of Least Privilege." Users are granted only the minimum level of access necessary to perform their assigned job functions. Access is not granted by default.

##2.2 Need-to-Know
Access to specific data is granted only to those individuals who have a legitimate business need to know that information.

##2.3 Separation of Duties
Where feasible, conflicting duties and responsibilities are separated to reduce the risk of unauthorized or unintentional modification or misuse of organizational assets.

#3. User Access Management

##3.1 Access Provisioning
- All requests for new access must be documented and approved by the Security Officer.
- Access is granted based on defined roles (Role-Based Access Control - RBAC) wherever possible.

##3.2 Access Modification
- Changes to user access rights (e.g., due to a role change) must be requested and approved following the same process as new access.

##3.3 Access Revocation (Termination)

- Access rights for terminated employees or contractors must be revoked immediately upon termination, and in no case later than 24 hours after the effective date/time.
- All Company-owned devices must be returned or remotely wiped.

##3.4 Access Reviews
- The Security Officer conducts a quarterly review of all user access rights to ensure they remain appropriate.
- Any access that is no longer required is promptly revoked.

#4. Authentication Standards

##4.1 Unique Identification
- Every user must have a unique user ID. Shared accounts are prohibited unless explicitly authorized for a specific technical requirement and strictly monitored.

##4.2 Password Policy
- **Minimum Length:** Passwords must be at least 12 characters long.
- **Complexity:** Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters.
- **History:** Passwords must not be reused for a minimum of 5 generations.
- **Storage:** Passwords must never be stored in plain text. They must be hashed and salted using industry-standard algorithms (e.g., bcrypt, Argon2).

##4.3 Multi-Factor Authentication (MFA)
- MFA is mandatory for all remote access and all access to production environments, including but not limited to:
  - Supabase (Database & Auth)
  - Vercel (Hosting)
  - Cloudflare (DNS & Security)
  - GitHub (Source Code)
  - AWS (Infrastructure)

#5. System Access Control

##5.1 Session Management
- Sessions must lock or time out after a defined period of inactivity (e.g., 15 minutes).
- Re-authentication is required to unlock the session.

##5.2 API Access
- API access must be authenticated using secure tokens or keys.
- API keys must be rotated periodically and immediately if compromise is suspected.

Data Management & Classification

Data Management & Classification Policy

#1. Overview

##1.1 Purpose

This policy defines the framework for classifying, handling, and protecting data assets based on their sensitivity and criticality to Craic Studio LLC. Proper classification ensures that appropriate security controls are applied to protect data from unauthorized disclosure, alteration, or destruction.

##1.2 Scope
This policy applies to all data created, received, processed, or stored by Craic Studio LLC, in any format.

#2. Data Classification Scheme

##2.1 Level 1: Public
Information that is intended for public release or is already publicly available. Disclosure causes no harm to the Company.
- *Examples:* Marketing materials, public website content, press releases.

##2.2 Level 2: Internal
Information intended for internal use within the Company. Unauthorized disclosure could cause minor operational disruption or embarrassment.
- *Examples:* Internal memos, non-sensitive project documentation, employee handbooks.

##2.3 Level 3: Confidential
Sensitive information that, if compromised, could cause significant financial, legal, or reputational harm. Access is strictly limited to authorized personnel.
- *Examples:* Personally Identifiable Information (PII), API keys, secrets, proprietary source code, client business strategies, financial records.

#3. Data Handling Requirements

##3.1 Encryption
- **Data in Transit:** All Confidential data transmitted over public networks must be encrypted using TLS 1.2 or higher.
- **Data at Rest:** All Confidential data stored in databases (Supabase), file storage, or backups must be encrypted using strong encryption standards (e.g., AES-256).

##3.2 Storage and Residency
- Client data must be stored in dedicated Supabase instances located within the United States.
- Logical separation must be maintained between different clients' data to prevent commingling.

##3.3 Data Retention and Disposal
- Data is retained only for as long as necessary to fulfill the purposes for which it was collected, or as required by law.
- Upon expiration of the retention period, data must be securely deleted or destroyed.
- Users have the right to request the deletion of their personal data, which the Company will honor in accordance with applicable privacy laws.

##3.4 Privacy and PII
- **Minimization:** We collect only the minimum amount of PII necessary for service delivery (e.g., names, email addresses, billing information).
- **Third-Party Sharing:** We do not sell user data. Data is shared only with critical infrastructure providers under strict Data Processing Agreements (DPAs).

- **Analytics & Communications:** We utilize specific third-party processors to improve our services and communicate with users:
  - **OneSignal:** Used for user analytics, push notifications, and email communications.
  - **Mixpanel:** Used for product analytics and user behavior tracking.
  - **Resend:** Used for transactional email delivery.
  - All third-party processors are vetted for security compliance (SOC 2, GDPR) and are bound by confidentiality agreements.

#4. Labeling and Handling
- Confidential information should be clearly labeled where feasible.
- When discussing Confidential information in public places, personnel must take care to prevent eavesdropping.
- Confidential documents must not be left unattended on printers or desks.

Software Development Lifecycle (SDLC)

Software Development Lifecycle (SDLC) Policy

#1. Overview

##1.1 Purpose
This policy mandates security integration into every phase of the software development lifecycle (SDLC) at Craic Studio LLC. The goal is to ensure that security is a core requirement, not an afterthought, and to minimize vulnerabilities in our software products.

##1.2 Scope
This policy applies to all software development projects managed by Craic Studio LLC, including internal tools, client projects, and SaaS products.

#2. Development Standards

##2.1 Secure Coding Guidelines
Developers must adhere to secure coding best practices, such as OWASP Top 10, to prevent common vulnerabilities (e.g., SQL Injection, XSS, CSRF).

##2.2 Version Control
- All source code must be managed in a version control system (GitHub).
- Repositories must be private by default.
- Branch protection rules must be enabled for the `main` or `production` branch to prevent direct commits.

#3. Review and Testing

##3.1 Code Review
- All code changes must undergo a peer review or lead developer review via Pull Request (PR) before merging into the production branch.
- Reviews must check for security flaws, logic errors, and adherence to coding standards.
- Automated AI-based code review tools may be used to assist but not replace human review.

##3.2 Vulnerability Scanning

- **Dependency Scanning:** We use automated tools (e.g., Snyk, GitHub Dependabot) to scan for known vulnerabilities in third-party libraries (npm packages).
- **Static Analysis (SAST):** Static Application Security Testing tools are integrated into the CI/CD pipeline to detect security issues in the code.

#4. Deployment

##4.1 Separation of Environments
- Development, Staging, and Production environments must be logically separated.
- Test data should be used in non-production environments whenever possible. If production data is used, it must be sanitized/anonymized.

##4.2 Change Management
- All changes to production must be documented and approved.
- Deployments should be automated via CI/CD pipelines (e.g., Vercel, GitHub Actions) to ensure consistency and reduce human error.

#5. Training
- Developers are required to complete secure coding training at least annually to stay current with emerging threats and defense techniques.

Incident Response Plan

Incident Response Plan

#1. Overview

##1.1 Purpose
The Incident Response Plan (IRP) defines the organized approach of Craic Studio LLC to addressing and managing the aftermath of a security breach or cyberattack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

##1.2 Scope
This plan applies to all security incidents involving Company information assets, systems, or data.

#2. Incident Response Team (IRT)

##2.1 Roles
- **Incident Commander:** Owner/Lead Developer. Responsible for overall coordination, decision-making, and communication.
- **Technical Lead:** Responsible for technical investigation, containment, and remediation.

#3. Incident Response Process

##3.1 Phase 1: Preparation
- Ensure monitoring and logging tools (Sentry, Cloudflare, Supabase) are active and configured correctly.
- Maintain and update this IRP.
- Conduct periodic drills or tabletop exercises.

##3.2 Phase 2: Identification
- Detect potential incidents through monitoring alerts, user reports, or system anomalies.
- **Triage:** The IRT investigates to determine if an event is a true security incident.
- **Classification:** Classify the incident severity:
  - *Low:* No impact on critical systems or data.
  - *Medium:* Localized impact, no sensitive data loss.
  - *High:* Significant impact, potential data loss or service disruption.
  - *Critical:* Major breach of sensitive data, massive financial or reputational impact.

##3.3 Phase 3: Containment
- **Short-term Containment:** Immediate actions to stop the spread (e.g., isolating a server, blocking an IP address, disabling a compromised account).
- **Long-term Containment:** Temporary fixes to allow operations to continue while the root cause is addressed.

##3.4 Phase 4: Eradication
- Identify the root cause of the incident.
- Remove the threat (e.g., delete malware, patch vulnerability, reset all compromised credentials).
- Verify that the threat has been completely eliminated.

##3.5 Phase 5: Recovery
- Restore systems to normal operation.
- Restore data from clean backups if necessary.
- Monitor systems closely for any signs of recurrence.

##3.6 Phase 6: Lessons Learned (Post-Mortem)
- Conduct a post-incident review meeting within 2 weeks of resolution.
- Document what happened, what went well, and what needs improvement.
- Update policies and procedures based on findings.

#4. Communication

##4.1 Internal Communication
- The Incident Commander keeps internal stakeholders informed of the status.

##4.2 External Communication
- **Clients:** Affected clients will be notified without undue delay, in accordance with contractual obligations and applicable laws.
- **Legal/Regulatory:** Legal counsel and regulatory bodies will be notified as required by law (e.g., GDPR, CCPA, state breach notification laws).

Vendor Management Policy

Vendor Management Policy

#1. Overview

##1.1 Purpose
This policy establishes the requirements for evaluating, selecting, and managing third-party vendors to

ensure that they meet Craic Studio LLC's security and compliance standards. Third-party risks must be managed to protect the Company's data and operations.

##1.2 Scope
This policy applies to all third-party vendors, service providers, and partners who have access to Company data or systems.

#2. Vendor Selection and Due Diligence

##2.1 Evaluation Criteria
Prior to engaging a new vendor, a security assessment must be performed. Factors to consider include:
- **Security Certification:** Does the vendor hold recognized certifications (e.g., SOC 2 Type 2, ISO 27001)?
- **Data Handling:** How does the vendor store, process, and protect data?
- **Reputation:** What is the vendor's history regarding security incidents?

##2.2 Critical Vendors
Our current critical infrastructure vendors have been vetted and hold industry-leading security certifications:
- **Supabase:** Database & Auth (SOC 2 Type 2, HIPAA compliant)
- **Vercel:** Hosting & Deployment (SOC 2 Type 2, ISO 27001)
- **Cloudflare:** Network Security & CDN (SOC 2 Type 2, PCI DSS)
- **Expo:** Mobile Development Platform
- **OneSignal:** Customer Engagement (SOC 2 Type 2, GDPR)
- **Mixpanel:** Product Analytics (SOC 2 Type 2, GDPR, CCPA)
- **Resend:** Email Infrastructure (SOC 2 Type 2, GDPR)

#3. Contractual Agreements
Contracts with vendors must include appropriate security and confidentiality clauses, including:
- Right to audit (where applicable).
- Data protection requirements.
- Notification requirements for security breaches.

#4. Ongoing Monitoring

##4.1 Annual Review
The Security Officer reviews the security posture of critical vendors at least annually. This may involve reviewing their latest SOC 2 reports or security whitepapers.

##4.2 Termination
Upon termination of a vendor relationship, the Company ensures that all Company data is securely returned or destroyed and that all access rights are revoked.

Business Continuity & Disaster Recovery

Business Continuity & Disaster Recovery Plan

#1. Overview

##1.1 Purpose
The purpose of this plan is to ensure that Craic Studio LLC can maintain or quickly resume critical business

functions in the event of a disaster or significant disruption. This includes natural disasters, technical failures, and cyberattacks.

##1.2 Scope
This plan covers all critical systems, applications, and data required for the Company's operations.

#2. Business Impact Analysis (BIA)
We have identified the following critical assets and their Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO):
- **Production Database (Supabase):** RTO < 4 hours, RPO < 1 hour.
- **Source Code (GitHub):** RTO < 4 hours, RPO < 24 hours.
- **Web Application (Vercel):** RTO < 1 hour.

#3. Data Backup Strategy

##3.1 Database Backups
- **Automated Backups:** Supabase performs automated daily backups of all production databases.
- **Point-in-Time Recovery (PITR):** PITR is enabled for critical production databases, allowing restoration to any second in the retention period.
- **Encryption:** All backups are encrypted at rest.

##3.2 Code Repositories
- Source code is hosted on GitHub, a distributed version control system. Every developer's machine serves as a redundant backup of the full codebase history.

#4. Disaster Recovery Procedures

##4.1 Database Failure
1. Assess the extent of the corruption or data loss.
2. Initiate restoration from the latest clean backup or use PITR via the Supabase dashboard.
3. Verify data integrity after restoration.
4. Update DNS or application configuration if the connection string changes.

##4.2 Hosting/Region Failure
1. Vercel's edge network automatically routes traffic away from failed regions.
2. In the event of a total provider failure, code can be redeployed to an alternative hosting provider (e.g., Netlify, AWS Amplify) from GitHub.

#5. Testing and Maintenance

##5.1 Testing
- Backup restoration procedures are tested at least annually to ensure that data can be successfully recovered within the defined RTO/RPO.
- Tabletop exercises are conducted to simulate disaster scenarios.

##5.2 Plan Update
This plan is reviewed and updated annually or following any significant change to the infrastructure.

Physical Security Policy

Physical Security Policy

#1. Overview

##1.1 Purpose
This policy outlines the physical security controls required to protect Craic Studio LLC's assets and personnel. As a remote-first company, this policy focuses on securing remote work environments and relying on cloud providers for data center security.

##1.2 Scope
This policy applies to all physical locations where Company work is performed, including home offices and co-working spaces.

#2. Remote Work Security

##2.1 Workspace Security
- Employees must ensure their remote workspace is secure.
- Computers must be locked when left unattended, even at home.
- Screens should be positioned to prevent "shoulder surfing" when working in public places.

##2.2 Asset Protection
- Company-issued devices must be kept secure from theft or damage.
- Lost or stolen devices must be reported to the Security Officer immediately to allow for remote wiping.

##2.3 Document Disposal
- Sensitive physical documents must be shredded before disposal. They must not be thrown in regular trash.

#3. Data Center Security

##3.1 Cloud Providers
Craic Studio LLC does not own or operate physical data centers. We rely on top-tier cloud service providers (Supabase/AWS, Vercel) to host our infrastructure. We verify that these providers maintain strict physical security controls, including:
- **Perimeter Security:** Fencing, barriers, and 24/7 security guards.
- **Access Control:** Biometric scanners, keycards, and mantraps.
- **Surveillance:** CCTV monitoring of all entry points and server rooms.
- **Environmental Controls:** Fire suppression, climate control, and redundant power systems.

#4. Visitor Policy
Since the Company operates remotely, there are no corporate offices for visitors. Any in-person meetings with clients or partners should be conducted in public venues or rented meeting spaces, where no sensitive Company data is left unsecured.