### Sicherheitsrichtlinien und -verfahren

| **Feld** | **Beschreibung** |
| --- | --- |
| **Name des Artefakts** | Sicherheitsrichtlinien und -verfahren |
| **Verantwortlich** | IT-Security-Spezialist |
| **Ziel des Dokuments** | Definition der Richtlinien und Verfahren zur Gewährleistung der IT-Sicherheit. |
| **Wesentliche Inhalte** | - Sicherheitsrichtlinien  - Sicherheitsverfahren  - Notfallpläne |
| **Erstellungszeitpunkt** | Anfangsphase des Projekts |
| **Nutzung im Projektverlauf** | Grundlage für die Implementierung und Überprüfung der Sicherheit der Anwendung |
| **Abnahme** | Durch den IT-Security-Spezialisten und die IT-Systemverantwortlichen; Überprüfung der Vollständigkeit und Korrektheit der Sicherheitsrichtlinien und -verfahren |
| **Abhängigkeiten** | - Sicherheitsanforderungen  - Technische Spezifikationen |
| **Versionierung** | Versionskontrolle mittels Versionsmanagement-Tools |
| **Vorlagen und Tools** | Textverarbeitungssoftware (z.B. MS Word, Google Docs) |
| **Zusätzliche Anmerkungen** | Regelmäßige Überprüfung und Aktualisierung der Sicherheitsrichtlinien und -verfahren notwendig, um sicherzustellen, dass sie den aktuellen Bedrohungen und Anforderungen entsprechen |

## Sicherheitsrichtlinien und -verfahren für die Erweiterung des CRM-Systems

### 1. Überblick

| **Feld** | **Beschreibung** |
| --- | --- |
| **Projektname** | Erweiterung des CRM-Systems um Scoring-Daten |
| **Projektleiter** | Max Mustermann |
| **IT-Sicherheitsverantwortlicher** | Laura Sicherheit |
| **Fachbereich** | Vertrieb |
| **Erstellungsdatum** | 19. Mai 2024 |
| **Version** | 1.0 |

### 2. Ziel

Das Ziel dieses Dokuments ist es, die Sicherheitsrichtlinien und -verfahren für die Erweiterung des bestehenden CRM-Systems festzulegen, um sicherzustellen, dass alle sicherheitsrelevanten Aspekte berücksichtigt und umgesetzt werden.

### 3. Sicherheitsrichtlinien

#### 3.1 Datenübertragung

| **Richtlinie** | **Beschreibung** |
| --- | --- |
| Verschlüsselte Übertragung | Alle Daten, die zwischen dem Benutzer und dem CRM-System übertragen werden, müssen über HTTPS verschlüsselt sein. |
| Vermeidung unsicherer Protokolle | Keine Verwendung von unsicheren Protokollen wie HTTP für die Datenübertragung. |

#### 3.2 Datenspeicherung

| **Richtlinie** | **Beschreibung** |
| --- | --- |
| Verschlüsselte Speicherung | Die Scoring-Daten müssen verschlüsselt in der Datenbank gespeichert werden. |
| Sicherstellung der Datenintegrität | Implementierung von Mechanismen zur Überprüfung und Sicherstellung der Datenintegrität. |

#### 3.3 Authentifizierung und Autorisierung

| **Richtlinie** | **Beschreibung** |
| --- | --- |
| Starke Authentifizierung | Benutzer müssen sich mit starken Authentifizierungsmethoden (z.B. 2-Faktor-Authentifizierung) anmelden. |
| Rollenbasierte Zugriffskontrolle | Der Zugriff auf die Scoring-Daten muss rollenbasiert gesteuert werden. |

#### 3.4 Audit und Protokollierung

| **Richtlinie** | **Beschreibung** |
| --- | --- |
| Protokollierung von Zugriffen | Alle Zugriffe auf die Scoring-Daten müssen protokolliert werden, einschließlich Benutzer-ID, Zeitstempel und Aktion. |
| Überwachung und Alarme | Ungewöhnliche Zugriffs- oder Aktivitätsmuster müssen erkannt und gemeldet werden. |

#### 3.5 Datenschutz

| **Richtlinie** | **Beschreibung** |
| --- | --- |
| Einhaltung der DSGVO | Alle Datenverarbeitungsprozesse müssen den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen. |
| Anonymisierung und Pseudonymisierung | Scoring-Daten müssen, wo immer möglich, anonymisiert oder pseudonymisiert werden, um den Datenschutz zu verbessern. |

### 4. Sicherheitsverfahren

#### 4.1 Datenübertragung

| **Verfahren** | **Beschreibung** |
| --- | --- |
| Implementierung von HTTPS | Einrichtung und Konfiguration von HTTPS für die sichere Datenübertragung. |
| Zertifikatsmanagement | Verwaltung und regelmäßige Erneuerung von SSL/TLS-Zertifikaten. |

#### 4.2 Datenspeicherung

| **Verfahren** | **Beschreibung** |
| --- | --- |
| Datenverschlüsselung | Verwendung von Verschlüsselungstechnologien wie AES zur Sicherung der gespeicherten Daten. |
| Integritätsprüfungen | Regelmäßige Überprüfung der Datenintegrität durch Hashing-Algorithmen und Integritätsprüfungen. |

#### 4.3 Authentifizierung und Autorisierung

| **Verfahren** | **Beschreibung** |
| --- | --- |
| Einrichtung der 2-Faktor-Authentifizierung | Implementierung einer 2-Faktor-Authentifizierungslösung (z.B. Google Authenticator, SMS-Verifizierung). |
| Verwaltung von Rollen und Rechten | Erstellung und Verwaltung von Benutzerrollen und Zugriffsrechten basierend auf dem Prinzip der minimalen Rechte. |

#### 4.4 Audit und Protokollierung

| **Verfahren** | **Beschreibung** |
| --- | --- |
| Protokollierung der Zugriffe | Implementierung von Logging-Mechanismen zur Erfassung von Zugriffen auf die Scoring-Daten. |
| Anomalieerkennung und Alarme | Einsatz von Überwachungstools zur Erkennung und Meldung ungewöhnlicher Zugriffs- oder Aktivitätsmuster. |

#### 4.5 Datenschutz

| **Verfahren** | **Beschreibung** |
| --- | --- |
| Datenschutzschulungen | Regelmäßige Schulungen der Mitarbeiter zu den Anforderungen der DSGVO und den Unternehmensrichtlinien zum Datenschutz. |
| Anonymisierung und Pseudonymisierung | Implementierung von Technologien und Verfahren zur Anonymisierung und Pseudonymisierung von Daten. |

### 5. Abnahmekriterien

* **Sicherheitstest**: Überprüfung, ob alle Daten verschlüsselt übertragen und gespeichert werden.
* **Penetrationstests**: Durchführung von Penetrationstests, um Sicherheitslücken zu identifizieren und zu schließen.
* **Zugriffskontrollen**: Überprüfung der Rollen- und Rechteverwaltung auf korrekte Implementierung.
* **Protokollierung**: Überprüfung der Vollständigkeit und Korrektheit der Zugriffprotokolle.

### 6. Risiken und Maßnahmen

| **Risiko** | **Maßnahme** |
| --- | --- |
| Datenlecks | Verschlüsselung der Datenübertragung und -speicherung, regelmäßige Sicherheitsüberprüfungen |
| Unbefugter Zugriff | Implementierung starker Authentifizierungsmethoden und rollenbasierter Zugriffskontrollen |
| Manipulation der Daten | Regelmäßige Integritätsprüfungen und Protokollierung aller Zugriffe |
| Datenschutzverstöße | Schulung der Mitarbeiter, Implementierung von Datenschutzrichtlinien und -verfahren |

### 7. Beteiligte Stakeholder

| **Stakeholder** | **Rolle** | **Verantwortlichkeiten** |
| --- | --- | --- |
| IT-Sicherheitsverantwortlicher | Sicherheitsmanagement | Festlegung und Überprüfung der Sicherheitsrichtlinien und -verfahren |
| Systemadministratoren | Technische Unterstützung | Implementierung und Wartung der Sicherheitsmaßnahmen |
| Vertriebsmitarbeiter | Endbenutzer | Nutzung des CRM-Systems und der neuen Scoring-Funktion |
| Vertriebsleiter | Führungskräfte | Analyse und Entscheidungsfindung basierend auf den Scoring-Daten |
| Datenschutzbeauftragter | Datenschutz | Sicherstellung der Einhaltung der Datenschutzbestimmungen |
| Projektleiter | Projektmanagement | Koordination und Überwachung des Projekts |

### 8. Dokumentation und Versionierung

| **Version** | **Datum** | **Beschreibung** |
| --- | --- | --- |
| 1.0 | 19. Mai 2024 | Initiale Version der Sicherheitsrichtlinien und -verfahren |
| 1.1 | XX.XXX.XXXX | Anpassungen basierend auf Feedback und neuen Erkenntnissen |

### 9. Vorlagen und Tools

* **Sicherheitsrichtlinien**: Unternehmensrichtlinien zur IT-Sicherheit.
* **Verschlüsselungstools**: Tools zur Datenverschlüsselung (z.B. OpenSSL, GPG).
* **Protokollierungstools**: Tools zur Überwachung und Protokollierung von Zugriffen (z.B. Splunk, ELK Stack).
* **Penetrationstests-Tools**: Tools zur Durchführung von Sicherheitstests (z.B. Metasploit, OWASP ZAP).