t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

Incident-Management-Prozess

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

1 Einführung und Überblick

Der Incident-Management-Prozess der Escola GmbH dient dazu, sicherzustellen, dass alle Vorfälle, die den Betrieb unserer Systeme und Dienstleistungen beeinträchtigen könnten, schnell und effizient behandelt werden. Der Prozess orientiert sich am ITIL4-Standard und zielt darauf ab, die Auswirkungen von Incidents zu minimieren und die Betriebsbereitschaft so schnell wie möglich wiederherzustellen. Dieser Prozess stellt sicher, dass die Escola GmbH jederzeit in der Lage ist, auf Vorfälle professionell zu reagieren und die Auswirkungen auf den Geschäftsbetrieb und der Kunden zu minimieren.

1.1 Zweck

- Schnelle Erkennung und Reaktion: Identifikation und schnelle Bearbeitung von Incidents, um die Auswirkungen auf den Betrieb zu minimieren.
- Effiziente Eskalation: Sicherstellung, dass Incidents, die nicht sofort gelöst werden können, an die richtigen Stellen eskaliert werden.
- Dokumentation und Nachverfolgung: Dokumentation der Incidents, um die Transparenz und Nachvollziehbarkeit zu gewährleisten.
- Kontinuierliche Verbesserung: Analyse der behandelten Incidents, um aus Fehlern zu lernen und zukünftige Vorfälle zu verhindern oder besser zu managen.

1.2 Ziele

- Minimierung von Ausfallzeiten: Durch schnelle und effektive Reaktion auf Incidents sollen Ausfallzeiten so kurz wie möglich gehalten werden.
- Erhöhung der Kundenzufriedenheit: Durch professionelle und transparente Bearbeitung von Incidents wird die Zufriedenheit unserer Kunden erhöht.
- Schutz der Unternehmensreputation: Durch effektives Incident Management wird das Vertrauen in unsere Systeme und Dienstleistungen gestärkt und unsere Reputation geschützt.
- Sicherstellung der Datenintegrität: Schutz sensibler Daten vor Verlust oder Beschädigung durch schnelle und gezielte Massnahmen bei Incidents.

1.3 Rollen

- Support
- Entwicklung
- Leitung Entwicklung
- Datenschutzverantwortlicher
- IT-Verantwortlicher
- Projektmanager

2 Identifikation

Der Service Desk nimmt Tickets, Telefonanrufe, E-Mails, App-Feedback und App-Rezensionen entgegen. Diese werden in die Kategorien Support, Feature Request, Management-Anfragen und Incidents eingestuft. Incidents werden vom Service Desk bearbeitet und gemäss definiertem Eskalationsprozess weitergeleitet.

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

Automatisierte Überwachungssysteme (unter anderem: Uptime Robot, Sentry, Trigger im Code, automatisierte Überprüfungsskripte, aktive Skriptüberwachung und ein eigenes Fehlererkennungstool) erkennen Incidents automatisch und eskalieren diese direkt an die Entwicklung.

3 Record

Incidents werden nach einem standardisierten Verfahren mit den folgenden Daten dokumentiert:

- Kennung
- Ersterfassung
- Art der Benachrichtigung
    - Tickets
    - Telefonanrufe
    - E-Mails
    - App-Feedback
    - App-Rezensionen
    - Überwachungstool
    - Manuelle Erkennung
- Service-Desk-Agent
- Melder-/ Anwenderdaten
- Kommunikationsweg für Rückmeldungen
- Symptombeschreibung
- Betroffenes Modul
- Priorisierung nach Dringlichkeit und Auswirkung (Legt die Reihenfolge fest, in der diese Probleme oder Aufgaben aufgrund ihrer Dringlichkeit und Auswirkung behandelt werden sollen)
- Kategorisierung als Major Incident (Bezieht sich auf die Schwere oder den Umfang des Incidents)
- Incident Categories
    - Datenintegrität und -sicherheit
    - Verfügbarkeit
    - Leistungsproblem
    - Software-Problem
- Links zu anderen Incident Records
- Lösungs- und Abschlussdaten
    - Lösung
    - Kunden-Feedback

4 Priorität

Alle Incidents werden nach der Dringlichkeit und Auswirkung kategorisiert. Daraus ergibt sich die Priorität zur Behandlung.

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

4.1 Dringlichkeit

- **Hoch**
  - Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit schnell zu.
  - Die Aufgaben, die von den Schulen nicht erfüllt werden können, sind sehr zeitkritisch.
  - Durch schnelles Handeln kann verhindert werden, dass aus einem Minor Incident ein Major Incident wird.
  - Datensicherheit ist gefährdet.
- **Mittel**
  - Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit substanziell zu.
  - Die Aufgaben, die von den Schulen nicht erfüllt werden können, sind nur mässig zeitkritisch.
- **Niedrig**
  - Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit nur unwesentlich zu.
  - Die Aufgaben, die von den Schulen nicht erfüllt werden können, sind nicht zeitkritisch.

4.2 Auswirkung

- **Hoch**
  - Eine grosse Anzahl von Schulen ist betroffen und/oder ist in irgendeiner Weise akuten Nachteilen ausgesetzt.
  - Eine grosse Anzahl von Mitarbeitenden ist betroffen und/oder kann ihre Aufgaben nicht erfüllen.
  - Eine Beschädigung der Reputation des Unternehmens in grossem Umfang ist wahrscheinlich.
- **Mittel**
  - Eine mässige Anzahl von Mitarbeitenden ist betroffen und/oder kann ihre Aufgaben nicht wie vorgesehen erfüllen.
  - Eine mässige Anzahl von Kunden ist betroffen und/oder erfährt Einschränkungen beim Komfort.
  - Eine Beschädigung der Reputation des Unternehmens in mässigem Umfang ist wahrscheinlich.
- **Niedrig**
  - Eine minimale Anzahl von Schulen ist betroffen und/oder erfährt Einschränkungen beim Komfort, jedoch nur in geringem Umfang
  - Eine minimale Anzahl von Mitarbeitenden ist betroffen und/oder kann ihre Aufgaben erfüllen, jedoch nur mit zusätzlichem Aufwand.
  - Eine Beschädigung der Reputation des Unternehmens ist nur in minimalem Umfang zu erwarten.

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

4.3 Priorität

		Dringlichkeit		
		H	M	N
Auswirkung	H	Kritisch	Hoch	Mittel
	M	Hoch	Mittel	Niedrig
	L	Mittel	Niedrig	Niedrig

5 Eskalation

5.1 Funktionale Eskalation

Technische Probleme werden nach folgender Eskalationshierarchie eskaliert:

1. **Level: Support**
    a. Erste Analyse und Identifikation des Incidents.
    b. Erfassung und Dokumentation des Incidents.
    c. Workarounds: Implementierung temporärer Lösungen zur Sicherstellung des Betriebs.
    d. Regelmässige Information relevanter Stakeholder über den Status und Fortschritt des Incidents.
    e. Eskalation von technischen Incidents an die Entwicklung.
    f. Eskalation von Major Incidents.
2. **Level: Entwicklung**
    a. Erkennung von Incidents durch automatisierte Überwachungssysteme.
    b. Analyse und Lösung von Incidents auf Code- und Datenbank-Ebene.
    c. Der Incident erfordert Anpassungen am Quellcode.
    d. Durchführung erweiterter Simulationen mit anonymisierten Produktivdaten.
    e. Sofortige Massnahmen zur Eindämmung des Incidents.
    f. Bereitstellung temporärer Lösungen, um den Betrieb aufrechtzuerhalten.
    g. Eskalation von besonders komplexen und zeitkritischen Incidents an die Leitung Entwicklung.
3. **Level: Leitung Entwicklung**
    a. Analyse und Lösung von Incidents auf Infrastruktur- oder Konfigurations-Ebene.
    b. Entscheidung und Implementierung von Änderungen an der IT-Infrastruktur und Systemkonfiguration.
    c. Analyse und Lösung besonders zeitkritischer und komplexer Incidents.

5.2 Management Eskalation

Bei weiterführenden Problemen oder wenn die Lösung des Incidents strategische Entscheidungen erfordert:

1. **Level: Support**
    a. Erste Analyse und Identifikation des Incidents.

b. Erfassung und Dokumentation des Incidents.
c. Workarounds: Implementierung temporärer Lösungen zur Sicherstellung des Betriebs.
d. Regelmässige Information relevanter Stakeholder über den Status und Fortschritt des Incidents.
e. Eskalation von technischen Incidents an die Entwicklung.
f. Eskalation von Major Incidents.

2. **Level: Zuständiger Projektmanager**
   a. Eingreifen bei Überschreitung von Service Level Agreements (SLAs).
   b. Behandlung besonders komplexer Incidents.
   c. Umgang mit unzufriedenen Kunden.
   d. Organisation und Koordination der erforderlichen Ressourcen zur Lösung langwieriger oder komplexer Incidents.
   e. Bewertung und Umsetzung notwendiger Änderungen am Produkt.
   f. Kommunikation mit externen Stakeholdern, Partnern und Kunden.
   g. Entscheid zur Notfallwiederherstellung von Gesamtsystemen oder Teilkomponenten.
3. **Level: Geschäftsleitung**
   a. Treffen von Entscheidungen mit strategischen Implikationen, die über den technischen Bereich hinausgehen.
   b. Initiierung und Überwachung von Massnahmen zur Bewältigung von Krisen.
   c. Management von Incidents mit besonders hohem Einfluss auf das Unternehmen.
   d. Entscheidungen zur Umsetzung von umfangreichen Produktänderungen.
   e. Umgang mit besonders unzufriedenen Kunden.

6 Major Incidents

6.1 Klassifikation von Major Incidents

Vorfälle, die einen erheblichen Einfluss auf die Systeme, Schulen und Geschäftsprozesse haben, müssen sofort an das Major Incident Team eskaliert werden. Dazu gehören unter anderem:

- Ausfall der gesamten Software.
- Verlust oder Korruption von Daten.
- Sicherheits- oder Datenschutzverletzungen.
- Akute Gefährdung der Sicherheit.
- Ausfälle, die mehrere Schulen betreffen.

6.2 Major Incident Team

- Hannes Bärtschi – Gründer, Inhaber, Datenschutzverantwortlicher
- Janick Pfenninger – Inhaber, IT-Verantwortlicher
- Florian Plattner – Leitung Entwicklung
- Noah Valley – Entwickler
- Lucas Schmidt – Entwickler
- Lars Hartmann – Projektmanager Entwicklung

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

7 Datenschutzvorfälle

Bei Datenschutzvofällen wird in jedem Fall der Datenschutzverantwortliche informiert. Der Datenschutzverantwortliche führt eine erste Bewertung des Vorfalls durch, um den Umfang und die Schwere des Vorfalls zu bestimmen. Schulen werden so schnell wie möglich informiert und auf mögliche gesetzlich vorgeschriebene Meldepflichten aufmerksam gemacht. Falls der Vorfall auf eine kriminelle Handlung hinweist, müssen auch die entsprechenden Strafverfolgungsbehörden informiert werden.

8 Notfallwiederherstellung

Die Entscheidung zur Notfallwiederherstellung von gesamten Systemen oder Teilkomponenten wird mindestens auf der Management-Eskalationsstufe 2 getroffen. Dabei werden die betroffenen Systeme sofort gesperrt, um den Datenverlust (Recovery Point Objective, RPO) zu minimieren. Bei der Wiederherstellung von Daten aus Backups, die innerhalb der letzten sieben Tage erstellt wurden, beträgt der Datenverlust ab der Incident-Erkennung maximal zwei Stunden (Backups alle zwei Stunden). Die Wiederherstellungsdauer eines Gesamtsystems beträgt ab der Incident-Erkennung und der anschliessenden Entscheidung zur Wiederherstellung eine Stunde. Die Wiederherstellungsdauer von Teilkomponenten variiert erheblich je nach Aufwand und wird fallbezogen geschätzt.

9 Service Level Agreements (SLA)

Service Level Agreements (SLA) sind ein integraler Bestandteil des Incident-Management-Prozesses der Escola GmbH. Sie definieren die erwarteten Reaktions- und Lösungszeiten für verschiedene Arten von Incidents und stellen sicher, dass unsere Dienstleistungen den vereinbarten Qualitätsstandards entsprechen. Weitere Informationen und Details zu unseren SLAs finden Sie hier: www.escola.ch/isms#sla.

10 Post-Incident Review (PIR)

Nach Abschluss eines Incidents wird bei Bedarf ein Post-Incident Review (PIR) mit dem gesamten Incident-Team durchgeführt, um Verbesserungsmöglichkeiten zu identifizieren. Bei Major Incidents ist die Durchführung eines PIR obligatorisch.

11 Schulung und Training

Regelmässige Schulungen für alle Mitarbeitenden stellen sicher, dass sie mit dem Incident-Management-Prozess vertraut sind. Diese Trainingsprogramme werden kontinuierlich durchgeführt, um sicherzustellen, dass alle Mitarbeitenden die notwendigen Kenntnisse und Fähigkeiten besitzen, um Incidents effektiv und effizient zu bearbeiten.

12 Tools und Technologien

- **Error Tracking**

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

- Sentry
- Escola-Adminkonsole

- **Perfomance Monitoring**
  - Sentry
  - Escola-Adminkonsole
- **Service Desk**
  - Freshdesk
  - Freshcaller
- **Projektmanagement**
  - Stackfield
- **Uptime Monitoring**
  - Uptime Robot
- **Überprüfungsskripts**
  - Escola-Adminkonsole
- **Script-Überwachung**
  - Escola-Adminkonsole

13 Kontinuierliche Verbesserung

Der Incident-Management-Prozess wird kontinuierlich weiterentwickelt und optimiert. Dabei werden die Erkenntnisse aus den Post-Incident Reviews (PIR) und den regelmässigen Incident-Reports sorgfältig analysiert. Diese Analysen helfen dabei, Schwachstellen zu identifizieren und Verbesserungsmöglichkeiten zu erkennen. Basierend auf diesen Erkenntnissen werden gezielte Anpassungen vorgenommen, um den Prozess effizienter und effektiver zu gestalten und auf neue Gegebenheiten und Herausforderungen flexibel reagieren zu können.

14 Verantwortlichkeiten

- **R** (Responsible):
  Verantwortlich für die Durchführung der Aufgabe.
- **A** (Accountable):
  Verantwortlich für das Endergebnis und die Entscheidungsfindung.
- **C** (Consulted):
  Eingebunden und konsultiert, um notwendige Informationen bereitzustellen.
- **I** (Informed):
  Wird über Fortschritte und Entscheidungen informiert.

t. 044 500 10 90
e. info@escola.ch
w. www.escola.ch

a. Escola GmbH
Beckenhofstrasse 72
8006 Zürich

Aufgabe	Support	Entwicklung	Leitung Entwicklung	Datenschutz-verantwortlicher	Projekt-manager	Geschäfts-leitung
Incident Identifikation	R					
Initiale Diagnose	R					
Priorisierung und Klassifizierung	R	C			C	
Funktionale Eskalation	R	A	I			
Management Eskalation	R				A	I
Incident Bearbeitung	R	C			C	
Incident Dokumentation	R	C	C	C	C	C
Lösung und Abschluss	R	R	C			
Unzufriedene Kunden					R	A
Post-Incident Review (PIR)	C	C	A	I	A	I
Datenschutzvorfälle				R, A		
Notfallwieder-herstellung		R			A	I
Kontinuierliche Verbesserung	R	R	A	I	R, A	I
Kommunikation während des Incidents	R				A	C
Einhaltung SLA	R				A	
Training und Schulung		A			A	C
Major Incident	I	C	R	C	R	A

Verantwortlichkeiten Escola GmbH