# Allgemeine Bedingungen und Regeln für die Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO/IEC 27001 und IT-Sicherheitskatalog

## 1 Allgemeines

Die Zertifizierungsstelle der Würth IT GmbH wurde nach DIN EN ISO IEC 17021-1:2015 unter der Verfahrensnummer D-ZM-18926-01 durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditiert. Die Zertifizierungsstelle der Würth IT GmbH bietet interessierten Unternehmen ihre Dienste zur Zertifizierung ihrer ISMS nach DIN EN ISO/IEC 27001:2017 und nach IT- Sicherheitskatalog gemäß § 11 Absatz 1a EnWG an.

## 2 Geltungsbereich

Diese Prüf- und Zertifizierungsordnung regelt die Zertifizierung von ISMS nach DIN EN ISO/IEC 27001:2017 und IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG durch die Zertifizierungsstelle der Würth IT GmbH.

## 3 Zertifizierungsverfahren

### 3.1 Voraussetzungen

Durch die schriftliche Annahme des Angebotes,

- schließt der Auftraggeber, nachfolgend Organisation genannt, einen Zertifizierungsvertrag mit der Zertifizierungsstelle der Würth IT GmbH
- erteilt er gleichzeitig damit einen Zertifizierungsauftrag
- erklärt er, dass keine weitere Zertifizierungsstelle mit der Durchführung des gleichen Verfahrens beauftragt wurde
- erkennt er diese Zertifizierungsbedingungen an.

### 3.2 Ablauf

Das Zertifizierungsverfahren auf Basis der DIN EN ISO/IEC 17021:2015 unterteilt sich in folgende Phasen:

### 3.2.1 Phase 1: Kundengespräch

Das Kundengespräch hat die Aufgabe, den Zertifizierungsverantwortlichen der Organisation über die Anforderungen der DIN EN ISO/IEC 27001:2017 zu unterrichten, den internen oder externen Auditoren Informationen über das Unternehmen zu vermitteln und die Interpretation der Norm aus Sicht der Zertifizierungsstelle im Rahmen einer Schulungsmaßnahme darzustellen. Des Weiteren werden die benötigten Auditaufwände kalkuliert und entsprechend aufgezeichnet.

Dabei erlangt die Organisation Kenntnis über die Erwartungshaltung der Zertifizierungsstelle und somit auch eine Entscheidungsgrundlage für die Fortführung des Verfahrens. Nach dem Kundengespräch hat die Organisation die Möglichkeit des Ausstiegs aus dem Verfahren ohne dass ihr zusätzliche Kosten entstehen.

### 3.2.2 Phase 2: Entwicklung und Einführung des ISMS

Die Organisation führt eine strukturierte Risikoanalyse durch. Bei dieser werden ihre materiellen und ideellen Werte erfasst und auf Schwachstellen hin analysiert. In einem weiteren Schritt zieht die Organisation daraus ihre Schlussfolgerungen und setzt diese in entsprechende Maßnahmen um.

Diese Maßnahmen werden unter Berücksichtigung der DIN EN ISO/IEC 27001:2017 eingeführt und entsprechend dokumentiert.

Die Dokumentation muss mindestens folgende Punkte umfassen:

- Die Aussagen des Managements in der Informationssicherheitspolitik
- Die Definition des Anwendungsbereiches
- Die Verfahren und Regelungen des ISMS-Handbuchs
- Die Beschreibung der angewandten Methodik bei der Risikoanalyse
- Die Ergebnisse aus der Risikoanalyse
- Der Plan zur Behandlung von Risiken
- Die Beschreibung des Prozesses zur Einführung und Aufrechterhaltung des ISMS
- Sicherheitsrelevante Aufzeichnungen, mindestens müssen die Ergebnisse aus dem internen Audit vorhanden sein, ebenso die Managementbewertung.
- Erklärung zur Anwendbarkeit der in der Norm geforderten Regelungen (Annex A)

### 3.2.3 Phase 3: Desktop Review

Die Organisation erläutert bei einem vor Ort Audit das ISMS und übergibt die Dokumentation an die Zertifizierungsstelle der Würth IT GmbH. Der leitende Auditor prüft daraufhin die Unterlagen auf Konformität mit der DIN EN ISO/IEC 27001:2017. Die Abweichungen werden in einem Abweichungsbericht erfasst, der dann an die Organisation zurückgesandt wird. Wurden keine Abweichungen festgestellt oder handelt es sich bei den festgestellten Abweichungen lediglich um geringfügige, also um Abweichungen, die eine Zertifizierung nicht unmöglich machen würden, kann

das Audit stattfinden. Die Vorlage der überarbeiteten Dokumente vor dem Audit ist nicht erforderlich. Bei erheblichen Abweichungen hat die Organisation 8 Wochen Zeit, um diese zu beseitigen, die Dokumentation entsprechend zu überarbeiten und die geänderte Fassung der Zertifizierungsstelle vorzulegen. Erst wenn die Zertifizierungsstelle keine erheblichen Abweichungen mehr feststellt, darf das Audit durchgeführt werden. Wird die 8-Wochen-Frist überschritten, so wird das Zertifizierungsverfahren durch die Zertifizierungsstelle der Würth IT GmbH vorübergehend geschlossen und der bis dahin entstandenen Aufwand mit der Organisation abgerechnet. Eine Wiederaufnahme des Verfahrens kann innerhalb eines halben Jahres ab dem Datum des Abweichungsberichts durch die Organisation beantragt werden, wenn sie gleichzeitig die erforderlichen Dokumente vorlegt. In diesem Fall wird das Desktop Review erneut in vollem Umfang durchgeführt. Nach Verstreichen der Halbjahresfrist ab dem Datum des Abweichungsberichts wird das Verfahren endgültig geschlossen. Im Bedarfsfall wäre dann ein neues Verfahren zu beantragen.

### 3.2.4 Phase 4: Zertifizierungsaudit

Der leitende Auditor versendet ca. 2 Wochen vor Beginn des Zertifizierungsaudits einen Auditplan. Dieser enthält Informationen über durchzuführende Tätigkeiten und den zeitlichen Ablauf. Die Organisation prüft daraufhin die Machbarkeit und kann dann evtl. Änderungswünsche einbringen, die dann je nach Möglichkeit und Machbarkeit berücksichtigt werden.

Während des Audits ist es Aufgabe der Organisation, die praktische Anwendung ihrer dokumentierten Verfahren zu demonstrieren und die Wirksamkeit ihrer Maßnahmen unter Beweis zu stellen. Zum Abschluss des Audits wird die Organisation im Rahmen eines Abschlussgesprächs über die Ergebnisse des Audits unterrichtet.

### 3.2.5 Phase 5: Berichterstellung und Zertifikatserteilung

Im Anschluss an das Audit werden die Abweichungen in einem Abweichungsbericht erfasst, der dann innerhalb von 4 Wochen an die Organisation gesandt wird.

Alle erkannten Abweichungen müssen kundenseitig auf Ihre Ursachen hin analysiert werden (Ursachenanalyse). Die Ergebnisse sind zu dokumentieren und der Zertifizierungsstelle mitzuteilen.

Wurden keine Abweichungen festgestellt oder handelt es sich bei den festgestellten Abweichungen lediglich um geringfügige, also um Abweichungen, die eine Zertifizierung nicht unmöglich machen würden, teilt die Organisation dem leitenden Auditor innerhalb weiterer 2 Wochen schriftlich mit, welche Maßnahmen sie treffen wird oder bereits getroffen hat um die Abweichungen zu beseitigen. Daraufhin empfiehlt der leitende Auditor die Erteilung des Zertifikats. Ein Nachaudit ist in diesem Fall nicht erforderlich.

Bei erheblichen Abweichungen hat die Organisation 8 Wochen Zeit, diese zu beseitigen, die Dokumentation entsprechend zu überarbeiten und die geänderte Fassung der Zertifizierungsstelle vorzulegen. Nach Ablauf dieser Zeit wird innerhalb weiterer 4 Wochen ein Nachaudit durchgeführt,

das sich auf die Bereiche beschränkt, in denen die erheblichen Abweichungen festgestellt wurden. Erst wenn die Auditoren keine erheblichen Abweichungen mehr feststellen, darf die Erteilung des Zertifikats vorgeschlagen werden.

Wird die 2- (bei geringfügigen Abweichungen) bzw. 8-Wochen-Frist (bei erheblichen Abweichungen) von der Organisation überschritten, so wird das Zertifizierungsverfahren durch die Zertifizierungsstelle der Würth IT GmbH vorübergehend geschlossen und der bis dahin entstandenen Aufwand mit der Organisation abgerechnet. Eine Wiederaufnahme des Verfahrens kann innerhalb eines halben Jahres ab dem Datum des Abweichungsberichts durch die Organisation beantragt werden, wenn sie gleichzeitig die erforderlichen Dokumente vorlegt. In diesem Fall wird das Zertifizierungsaudit erneut in vollem Umfang durchgeführt. Nach Verstreichen der Halbjahresfrist ab dem Datum des Abweichungsberichts wird das Verfahren endgültig geschlossen. Im Bedarfsfall wäre dann ein neues Verfahren zu beantragen.

Nach positiver Prüfung der Dokumentation des Zertifizierungsverfahrens wird das Zertifikat durch den Leiter der Zertifizierungsstelle oder seines Stellvertreters erteilt. Die Entscheidung basiert auf der Grundlage der Beurteilung der Auditfeststellungen und Schlussfolgerungen sowie weiterer relevanter Informationen. Das Zertifikat wird nur erteilt, wenn alle erheblichen Abweichungen behoben sind.

Das Eigentumsrecht am Auditbericht und am Zertifikat bzw. an den Zertifikaten bleibt bei der Zertifizierungsstelle.

### 3.2.6 Phase 6: Überwachung

Die Gültigkeitsdauer des Zertifikates beträgt drei Jahre, wenn jährlich eine Überwachungsmaßnahme bei der Organisation durchgeführt wird. Die Überwachungsmaßnahme soll wenn möglich durch ein Vor-Ort-Audit erfolgen. Nach Ablauf des Zertifikats wird ein Re-Zertifizierungsaudit durchgeführt. In dem Jahr, in dem das Re-Zertifizierungsaudit durchgeführt wird, ist keine weitere Überwachungsmaßnahme erforderlich. Für die Aufrechterhaltung des Zertifikats gelten die Regeln für die Erstzertifizierung analog.

Die Überwachungstätigkeiten können Folgendes beinhalten:

- Anfragen der Zertifizierungsstelle an zertifizierte Kunden zu Aspekten der Zertifizierung;
- Bewertung der Angaben des Kunden im Hinblick auf seine Tätigkeiten;
- Aufforderungen an den Kunden zur Bereitstellung von Dokumenten und Aufzeichnungen und
- andere Mittel zur Überwachung der Leistungsfähigkeit des zertifizierten Kunden.

## 4 Zertifikats- und Zeichennutzung

Die Berechtigung zur Nutzung des Zertifikates durch die Organisation, beispielsweise für Marketingzwecke, beschränkt sich auf den im Zertifikat benannten Geltungsbereich. Des Weiteren muss bei der Nutzung die Rückverfolgbarkeit zur Zertifizierungsstelle gewährleistet sein. Es darf keine

Mehrdeutigkeit, in Bezug auf den Geltungsbereich und die Zertifizierungsstelle, welche die Zertifizierung gewährt hat, im Zeichen oder im dazugehörigen Begleittext bestehen. Das Zeichen der Zertifizierungsstelle darf nicht auf Produkten oder Produktverpackungen verwendet werden, die von Verbrauchern gesehen werden können oder in irgendeiner anderen Art und Weise verwendet werden, die als Kennzeichnung für Produktkonformität interpretiert werden könnten.

Die Organisation verpflichtet sich:

- die hier genannten Anforderungen bei einem Verweis auf ihren Zertifizierungsstatus in Kommunikationsmedien einzuhalten;
- keine irreführenden Angaben bezüglich der Zertifizierung zu machen oder zu gestatten;
- Zertifizierungsdokumente oder Teile davon nicht in irreführender Weise zu verwenden oder deren Verwendung zu gestatten;
- bei Aussetzung oder Entzug der Zertifizierung die Verwendung aller Werbematerialien zu beenden, welche Verweise auf den Zertifizierungsstatus enthalten;
- bei Reduzierung des Geltungsbereichs der Zertifizierung die Werbematerialien dementsprechend abzuändern;
- keinen Verweis auf die Managementsystemzertifizierung zuzulassen, der stillschweigend andeuten könnte, dass die Zertifizierungsstelle ein Produkt (einschließlich einer Dienstleistung) oder einen Prozess zertifiziert oder nicht stillschweigend andeutet, dass die Zertifizierung für Tätigkeiten gilt, die außerhalb des Geltungsbereichs der Zertifizierung liegen;
- keine Zeichen der Zertifizierungsstelle auf Laborprüfberichten, Kalibrierscheinen, Inspektionsberichten oder Zertifikaten anzuwenden;
- die Zertifizierung nicht in einer Art und Weise zu verwenden, welche die Zertifizierungsstelle und/oder das Zertifizierungssystem in Misskredit bringt und das öffentliche Vertrauen verliert.

Ein Zertifikat erlischt, wenn

- die im Zertifikat genannte Gültigkeitsdauer überschritten ist
- die Organisation auf das Zertifikat vor Ablauf der im Zertifikat genannten Gültigkeitsdauer verzichtet
- der Vertrag über die Zertifizierung von der Organisation gekündigt wird
- die dem Zertifikat zugrunde gelegten Bestimmungen geändert wurden oder andere Bestimmungen, z. B. aufgrund geänderter Nutzung, anzuwenden sind.

Ein Zertifikat kann von der Zertifizierungsstelle zurückgezogen, wenn

- schwerwiegende Abweichungen festgestellt werden
- die Organisation die vereinbarten Überprüfungen ihres ISMS durch die Zertifizierungsstelle oder deren beauftragte prüfende Stelle nicht zulässt oder behindert
- in Zusammenhang mit dem Zertifikat irreführende oder anderweitig unzulässige Werbung betrieben wird

- aufgrund von Tatsachen, die einer Zertifizierung entgegenstehen würden, die zum Zeitpunkt der Zertifikatserteilung nicht zu erkennen waren.

Die Zertifizierungsstelle kann das Erlöschen oder die Zurückziehung nach eigener Wahl veröffentlichen.

Die Zertifizierungsstelle ist berechtigt, die Aufsichtsbehörden, die Akkreditierungsstellen, andere Zertifizierungsstellen und die Zulassungsbehörden über das Erlöschen oder die Zurückziehung von Zertifikaten zu informieren.

Die Zertifizierungsstelle haftet nicht für Nachteile, die der Organisation aus der Nichterteilung, dem Erlöschen oder der Zurückziehung eines Zertifikats erwachsen.

Ein Zertifikat kann ausgesetzt werden, wenn

- die Zertifizierungsanforderungen, einschließlich der Anforderungen an die Wirksamkeit des ISMS, dauerhaft oder schwerwiegend nicht erfüllt werden
- der zertifizierte Kunde die Durchführung der Überwachungs- oder Re-Zertifizierungsaudit nicht gestattet
- der zertifizierte Kunde freiwillig um eine Aussetzung gebeten hat.

Im Falle einer Aussetzung des Zertifikats ist die Managementsystemzertifizierung zeitweise außer Kraft gesetzt. Hierbei ist es der Organisation untersagt, weiterhin für ihre Zertifizierung zu werben.

Werden die Ursachen, welche zur Aussetzung des Zertifikats geführt haben, nicht in einem von der Zertifizierungsstelle vorgegebenen Zeitraum gelöst, führt dies zu einer Zurückziehung oder Einschränkung des Geltungsbereiches der Zertifizierung. Die Einschränkung des Geltungsbereiches schließt diejenigen Teile aus, welche den Anforderungen nicht genügen und steht in Übereinstimmung mit den Anforderungen der für die Zertifizierung verwendeten Norm.

Die Zertifizierungsstelle ist berechtigt, das Aussetzen der Zertifizierung zu veröffentlichen und weitere, als angemessen erachtete, Maßnahmen zu ergreifen.

Die Zertifizierungsstelle veröffentlicht auf ihrer Internetseite des Certification Center Security (kurz ccSec) den Namen, Geltungsbereich, geographischen Standort (Stadt und Land), Status der Zertifizierung und einen Link zur Webseite der zertifizierten Kunden.

## 5 Pflichten von der Zertifizierungsstelle der Würth IT GmbH

Die Zertifizierungsstelle der Würth IT GmbH verpflichtet sich, alle ihr zugänglich gemachten Informationen über das Unternehmen des Auftraggebers vertraulich zu behandeln und nur für den vereinbarten Zweck auszuwerten. Zugänglich gemachte Unterlagen werden nicht an Dritte weitergegeben. Hiervon ausgeschlossen ist die ausführliche Berichterstattung an die Schiedsstelle in Streitfällen. Der Kunde kann die Zertifizierungsstelle aus bestimmten Gründen von dieser Pflicht entbinden.

Änderungen an den Zertifizierungsanforderungen werden der Organisation rechtzeitig bekanntgegeben.

Ergänzend zu unseren allgemeinen Geschäftsbedingungen und als notwendige Vertragsbedingung, beschränkt sich die Haftung von der Zertifizierungsstelle der Würth IT GmbH gegenüber der Organisation oder Dritten auf die gesetzliche Mindestforderung im Falle eines Vorsatzes oder grober Fahrlässigkeit. Weitergehende Ansprüche sind ausgeschlossen. Dies gilt insbesondere für die Durchführung von Netzwerkanalysemaßnahmen.

## 6 Pflichten der Organisation

Folgende Pflichten sind von der Organisation vor, während und nach dem Zertifizierungsverfahren zu erfüllen:

- Bereitstellung geeigneter Arbeitsplätze für die Auditoren während der Audits
- Ggf. Bereitstellung geeigneter Netzzugänge für die Durchführung von Netzwerkanalysen
- Bereitstellung kompetenter Interviewpartner während den Interviews
- Bereitstellung der erforderlichen Dokumentation
- Einhaltung von neuen Zertifizierungsanforderungen (im Falle von Änderungen)
- Mitteilung von Änderungen bezüglich
    - der Rechts- oder Organisationsform der wirtschaftlichen oder der Besitzverhältnisse
    - Organisation und Management
    - Kontaktadressen und Standorte
    - des erfassten Tätigkeitsfeldes
    - wesentlicher Veränderungen des Managementsystems sowie der Prozesse

## 7 Einspruchsverfahren

Die Organisation kann vor dem Audit Einspruch gegen die Auditoren einlegen, die während des Audits eingesetzt werden sollen. Diese werden ihr ca. 2 Wochen vor dem Audit von der Zertifizierungsstelle der Würth IT GmbH mitgeteilt. Im Falle eines Einspruchs der Organisation gegen einen oder mehrere Auditoren prüft der LZ, ob Alternativen möglich sind bzw. das Audit dennoch durchführbar ist. Danach bespricht er die weitere Vorgehensweise mit der Organisation. Für vertragsrechtliche Folgen gelten die gesetzlichen Bestimmungen.

Die Organisation kann auch Einspruch bzw. Beschwerde gegen sonstige nicht zufriedenstellende Entscheidungen der Zertifizierungsstelle im Rahmen des durchgeführten Zertifizierungsverfahrens

bei der Zertifizierungsstelle erheben. Die Zertifizierungsstelle begründet daraufhin der Organisation die Entscheidung, soweit noch nicht erfolgt, nochmals ausführlich, ggf. mit Verweisen auf die relevanten Stellen in der Projektdokumentation.

Ist die Begründung der Zertifizierungsstelle für die Organisation nicht nachvollziehbar oder akzeptiert sie diese nicht, so kann sie eine Beschwerde beim Lenkungsausschuss der Zertifizierungsstelle einlegen. Der Lenkungsausschuss trifft dann die endgültige Entscheidung.

## 8 Witness-Audits durch die Akkreditierungsstelle

Die Organisation duldet im Bedarfsfall die Begleitung der Zertifizierungsstelle der Würth IT GmbH - Auditoren durch Begutachter der DAkkS (Deutsche Akkreditierungsstelle).

## 9 Inkrafttreten

Diese Zertifizierungsregeln treten am 11.10.2022 in Kraft. Sie gelten grundsätzlich für alle Zertifikate, die im Zeitraum der Gültigkeit durch die Zertifizierungsstelle der Würth IT GmbH erteilt werden. Zukünftige Änderungen können auf bestehende Zertifikate nur nach schriftlichem Einverständnis mit den Inhabern angewendet werden.

Ulrike Schröder

Leiterin der Zertifizierungsstelle der Würth IT GmbH, ccSec