Selbsterklärung der prüfenden Stelle

Name der prüfenden Stelle: _____

ID des geprüften Betreibers: _____

Die prüfende Stelle erklärt hiermit, dass sie folgende Eignungsvoraussetzungen (A) erfüllt und die ethischen Grundsätze (B) einhält

A. Eignungsvoraussetzungen

- Die zur Durchführung der Prüfung erforderlichen Prozesse (z. B. Informationssicherheitsmanagementsystem (ISMS), Qualitätssicherungsverfahren, Dokumentations- und Aufzeichnungsverfahren, Archivierungs- und Backupkonzept, Prüfprozess) sind eingeführt, umgesetzt und in Konzepten dokumentiert.
- Die prüfende Stelle gewährleistet, dass jede Prüfung nach einem dokumentierten Prüfprozess durchgeführt wird. Das einheitliche Verständnis von Abweichungen ist für die Bewertung der Mängel zwingend erforderlich. Wird ein Sicherheitsmangel als schwerwiegende Abweichung bewertet, werden die Ursachen analysiert und nachvollziehbar dokumentiert.
- Es ist sichergestellt, dass die Prüfung unabhängig und unparteilich, neutral und weisungsfrei erfolgt.
- Die Art und der Umfang der Prüfungshandlungen und -ergebnisse werden einheitlich, sachlich und ordnungsgemäß dokumentiert.
- Es werden ausreichend kompetente Personen und geeignete Infrastrukturen zur Verfügung gestellt. Die prüfende Stelle
    - verfügt über mindestens eine/-n Leiter/-in und eine/-n Stellvertreter/-in, um geplante und ungeplante Ausfälle der Leitung kompensieren zu können,
    - ist in der Lage, das Prüfungsverfahren in einer angemessenen Zeit durchzuführen,
    - verfügt nachweislich über eine sichere Infrastruktur, Systeme, Anwendungen und eine sichere IT-Netzstruktur.
- Die prüfende Stelle verfügt über einen festgelegten Prozess zur Ermittlung der Kompetenz des Prüfteams.
- Zur Durchführung der Prüfung sind folgende Kompetenzen im Prüfteam vorhanden:
    - belastbares Wissen im Bereich der Informationssicherheit,
    - Branchenkenntnisse und technisches Wissen im Bereich der Erbringung der kritischen Dienstleistungen der geprüften KRITIS-Betreiber,
    - belastbares Wissen im Bereich Managementsysteme und insbesondere Informationssicherheitsmanagementsysteme (ISMS),
    - detaillierte Kenntnisse der Anforderungen an Prüfungen nach § 8a Absatz 3 BSIG.

B. Ethische Grundsätze

Rechtschaffenheit und Vertrauenswürdigkeit

Die Rechtschaffenheit begründet Vertrauen und schafft damit die Grundlage für die Zuverlässigkeit eines Urteils. Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Informationen zu finden sind, ist die Vertraulichkeit der während einer Prüfung erlangten Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der Prüfung eine wichtige Arbeitsgrundlage. Prüfer/-innen beachten den Wert und das Eigentum der erhaltenen Informationen und legen diese nicht ohne entsprechende Befugnis offen, es sei denn, es bestehen dazu rechtliche oder berufliche Verpflichtungen.

Fachkompetenz

Prüfer/-innen übernehmen nur solche Aufgaben, für die sie das erforderliche Wissen, Können und die entsprechende Erfahrung haben und setzen diese bei der Durchführung ihrer Arbeit ein. Sie verbessern kontinuierlich ihre Fachkenntnisse sowie die Effektivität und Qualität ihrer Arbeit.

Objektivität und Sorgfalt

Ein Prüfer/eine Prüferin hat ein Höchstmaß an sachverständiger Objektivität und Sorgfalt beim Zusammenführen, Bewerten und Weitergeben von Informationen über geprüfte Aktivitäten oder Geschäftsprozesse zu zeigen. Die Beurteilung aller relevanten Umstände hat mit Ausgewogenheit zu erfolgen und darf nicht durch eigene Interessen oder durch Andere beeinflusst werden.

Sachliche Darstellung

Ein Prüfer/eine Prüferin hat die Pflicht, seinem/ihrem Auftraggeber wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehören die objektive und nachvollziehbare Darstellung der Sachverhalte in den Prüfberichten, die konstruktive Bewertung der dargestellten Sachverhalte und die konkreten Empfehlungen zur Verbesserung der Maßnahmen und Prozesse.

Nachweise und Nachvollziehbarkeit

Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Schlussfolgerungen und Ergebnissen zu kommen, ist die eindeutige und folgerichtige Dokumentation der Sachverhalte. Hierzu gehört auch eine dokumentierte und nachvollziehbare Methodik (Prüfplan, Bericht), mit der das Prüfteam zu seinen Schlussfolgerungen kommt.

Unabhängigkeit und Neutralität

Ein Prüfer/eine Prüferin muss weisungsfrei und unvoreingenommen die Prüfung durchführen. Er/sie muss die Prüfungsergebnisse nachvollziehbar dokumentieren können. Jedes Prüfteam sollte zur Gewährleistung der Unabhängigkeit und Objektivität aus mindestens zwei Prüfern bestehen („Vier-Augen-Prinzip“). Alle Mitglieder des Teams dürfen aus Gründen der Unabhängigkeit und Neutralität vorher nicht unmittelbar im geprüften Bereich beratend oder auch ausführend, z. B. bei der Erstellung von Konzepten oder Konfiguration von IT-Systemen, tätig gewesen sein.

_____	_____
Ort	Datum
_____	_____
Name in Druckbuchstaben	Unterschrift der prüfenden Stelle (zur Unterschrift berechtigte Person)