Verpflichtungserklärung zur Einhaltung der Sicherheitsrichtlinien nach IT Quality Circle

Mit der Unterzeichnung der Verpflichtungserklärung, erklärt sich Name der Organisation, die Einhaltung der gelisteten Verpflichtungen nach IT Quality Circle, ab dem Datum, und diese immer in der aktuellen Version einzuhalten.

Mit der Einhaltung der Anforderungen, ist das Unternehmen ebenfalls dazu berechtigt, das Label zu führen.

Nach Beendigung des Geschäftsverhältnisses, sind alle Unterlagen zurückzugeben.

Verpflichtung	
10101	Die Organisation verpflichtet sich, eine Richtlinie zu verabschieden und unterstützende Sicherheitsmaßnahmen umzusetzen, um die Risiken, die durch die Nutzung von mobilen Endgeräten bedingt sind, zu handhaben.
10201	Die Organisation verpflichtet sich, dass ein Verfahren für die Handhabung von Wechseldatenträgern entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema umgesetzt wurde.
10202	Die Organisation verpflichtet sich, dass nicht mehr benötigte Datenträger sicher und unter Anwendung formaler Verfahren entsorgt werden.
10203	Die Organisation verpflichtet sich , dass Datenträger, die Information enthalten, während des Transports vor unbefugtem Zugriff, Verfälschung oder Missbrauch geschützt werden.
10301	Die Organisation verpflichtet sich, eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Informationen, auf die von Homeoffice-Arbeitsplätzen aus zugegriffen werden oder die dort verarbeitet oder gespeichert werden, zu verabschieden und umzusetzen.
10401	Die Organisation verpflichtet sich, dass ein Verfahren zur Steuerung der Installation von Software auf Systemen im Unternehmen umgesetzt wird.
10402	Die Organisation verpflichtet sich, zur Festlegung und Umsetzung von Regeln, zur Softwareinstallation durch Benutzer.
10501	Die Organisation verpflichtet sich, ein Satz Informationssicherheitsrichtlinien festzulegen, die von der Leitung genehmigt, herausgegeben und den Beschäftigten, sowie relevanten externen Parteien bekanntgemacht werden.
10502	Die Organisation verpflichtet sich, die Informationssicherheitsrichtlinien in geplanten Abständen oder jeweils nach erheblichen Änderungen zu überprüfen, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.

10601	Die Organisation verpflichtet sich, dass alle Informationssicherheitsverantwortlichkeiten festgelegt und zugeordnet sind.
10602	Die Organisation verpflichtet sich, dass miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche getrennt werden, um die Möglichkeiten zu unbeabsichtigter oder unbefugter Änderung oder zum Missbrauch der Werte der Organisation reduzieren zu können.
10603	Die Organisation verpflichtet sich, dass angemessene Kontakte mit relevanten Behörden gepflegt werden.
10604	Die Organisation verpflichtet sich, dass angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheits-orientierten Expertenforen und Fachverbänden gepflegt werden.
10605	Die Organisation verpflichtet sich, dass Informationssicherheit im Projektmanagement berücksichtigt wird, unabhängig von der Art des Projekts.
10606	Die Organisation verpflichtet sich, dass es eine Mindestanforderung gibt, an die Dokumentation eines jeden Kunden, die als folgende Produkte als Managed-Version angeboten werden: • Monitoring • Patching • Backup • Firewall • SPAM-Filter • Fernwartung
10607	Die Organisation verpflichtet sich, dass mindestens 3 Techniker im Unternehmen vorhanden sind.
10608	Die Organisation verpflichtet sich, dass Produkte immer von min. zwei Techniker betreut werden.
10701	Die Organisation verpflichtet sich, dass alle Personen, die sich um eine Beschäftigung bewerben, einer Sicherheitsüberprüfung unterzogen werden, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen, sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken ist.
10702	Die Organisation verpflichtet sich, in den vertraglichen Vereinbarungen mit Beschäftigten und Auftragnehmern, deren Verantwortlichkeiten und diejenigen der Organisation festzulegen.
10703	Die Organisation verpflichtet sich, dass die Leitung von allen Beschäftigten und Auftragnehmern verlangt, dass sie die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umsetzen.
10704	Die Organisation verpflichtet sich, alle Beschäftigten der Organisation und ggf., Auftragnehmer, ein angemessenes Bewusstsein durch Ausbildung und Schulung zu vermitteln, sowie regelmäßige Aktualisierungen zu den

	Richtlinien und Verfahren der Organisation, die für ihr berufliches Arbeitsgebiet relevant sind, mitzuteilen.
10705	Die Organisation verpflichtet sich, dass ein formal festgelegter und bekanntgegebener Maßregelungsprozess eingerichtet ist, um Maßnahmen gegen Beschäftigte zu ergreifen, die einen Informationssicherheitsverstoß begangen haben.
10706	Die Organisation verpflichtet sich, Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, festzulegen, dem Beschäftigten oder Auftragnehmer mitzuteilen und durchzusetzen.
10801	Die Organisation verpflichtet sich, für alle Werte, die im Inventar geführt werden, Zuständige zu benennen.
10802	Die Organisation verpflichtet sich, dass Regeln für den zulässigen Gebrauch von Information und Werten, die mit Information und informationsverarbeitenden Einrichtungen in Zusammenhang stehen, aufgestellt, dokumentiert und angewendet werden.
10803	Die Organisation verpflichtet sich, sicherzustellen, dass alle Beschäftigte und sonstige Benutzer, die zu externen Parteien gehören, bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung, sämtliche in ihrem Besitz befindlichen Werte, die der Organisation gehören, zurückgeben.
10901	Die Organisation verpflichtet sich, eine Zugangssteuerungsrichtlinie auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen zu erstellen, dokumentieren und zu überprüfen.
10902	Die Organisation verpflichtet sich, dass Benutzer ausschließlich Zugang erhalten, zu denjenigen Netzwerken und Netzwerkdiensten, zu deren Nutzung sie ausdrücklich befugt sind.
10903	Die Organisation verpflichtet sich, zur Umsetzung eines formalen Prozesses, für die Registrierung und Deregistrierung von Benutzern, um die Zuordnung von Zugangsrechten zu ermöglichen.
10904	Die Organisation verpflichtet sich, zur Umsetzung eines formalen Prozesses, zur Zuteilung von Benutzerzugängen, um die Zugangsrechte für alle Arten von Benutzern zu allen Systemen und Diensten zuzuweisen oder zu entziehen.
10905	Die Organisation verpflichtet sich, die Zuteilung und den Gebrauch von privilegierten Zugangsrechten einzuschränken und zu steuern.
10906	Die Organisation verpflichtet sich, dass die Zuordnung von geheimer Authentisierungsinformation, über einen formalen Verwaltungsprozess gesteuert wird.
10907	Die Organisation verpflichtet sich, in regelmäßigen Abständen die Benutzerzugangsrechte zu überprüfen, durch die jeweiligen Zuständigen der Werte.

10908	Die Organisation verpflichtet sich, dass die Zugangsrechte aller Beschäftigten und Benutzer, die zu externen Parteien gehören, auf Information und informationsverarbeitende Einrichtungen, bei Beendigung des Beschäftigungsverhältnisses, des Vertrages oder der Vereinbarung entzogen oder bei einer Änderung angepasst werden.
10909	Die Organisation verpflichtet sich, dass Benutzer dazu verpflichtet werden, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.
10910	Die Organisation verpflichtet sich, die Speicherung der Passwörter in einem "sicheren"/verschlüsselten Passwortspeicher durchzuführen. • Keine Excel-Liste • Keine Datenbank die ein Mitarbeiter beim Ausscheiden mitnehmen kann
10911	Die Organisation verpflichtet sich, den Zugang zu Information und Anwendungssystemfunktionen einzuschränken, entsprechend der Zugangssteuerungsrichtlinie.
10912	Die Organisation verpflichtet sich, dass der Zugang zu Systemen und Anwendungen durch ein sicheres Anmeldeverfahren gesteuert wird, soweit es die Zugangssteuerungsrichtlinie erfordert.
10913	Die Organisation verpflichtet sich, Systeme zur Verwaltung von Kennwörtern einzusetzen, welche interaktiv sind und durch starke Kennwörter gesichert sind.
10914	Die Organisation verpflichtet sich, dass der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, eingeschränkt und streng überwacht ist.
10915	Die Organisation verpflichtet sich, den Zugang zu Quellcode von Programmen einzuschränken.
11001	Die Organisation verpflichtet sich, eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information zu entwickeln und umzusetzen.
11002	Die Organisation verpflichtet sich, eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln zu entwickeln und über deren gesamten Lebenszyklus umzusetzen.
11101	Die Organisation verpflichtet sich, dass zum Schutz von Bereichen, in denen sich entweder sensible oder kritische Information oder informationsverarbeitende Einrichtungen befinden, Sicherheitsperimeter festgelegt und verwendet werden.
11102	Die Organisation verpflichtet sich, die Sicherheitsbereiche durch eine angemessene Zutrittssteuerung, zu schützen, um sicherzustellen, dass nur berechtigtes Personal Zugang erhält.

11103	Die Organisation verpflichtet sich, dass die physische Sicherheit für Büros, Räume und Einrichtungen konzipiert und angewendet wird.
11104	Die Organisation verpflichtet sich, dass der physische Schutz vor Unfällen, Naturkatastrophen oder bösartigen Angriffen konzipiert und angewendet wird.
11105	Die Organisation verpflichtet sich, dass ein Verfahren für das Arbeiten in Sicherheitsbereichen, konzipiert und angewendet wird.
11106	Die Organisation verpflichtet sich, dass Zutrittsstellen wie Anlieferungs- und Ladebereiche sowie andere Stellen, über die unbefugte Personen die Räumlichkeiten betreten könnten, überwacht werden und, falls möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unbefugten Zutritt verhindern zu können.
11201	Die Organisation verpflichtet sich, Geräte und Betriebsmittel so zu platzieren und zu schützen, dass Risiken durch umweltbedingte Bedrohungen und Gefahren, sowie Möglichkeiten des unbefugten Zugangs verringert werden.
11202	Die Organisation verpflichtet sich, Geräte und Betriebsmittel vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, zu schützen.
11203	Die Organisation verpflichtet sich, die Telekommunikationsverkabelung, welche Daten trägt oder Informationsdienste unterstützt, und die Stromverkabelung vor Unterbrechung, Störung oder Beschädigung geschützt.
11204	Die Organisation verpflichtet sich, Geräte und Betriebsmittel instand zu halten, um ihre fortgesetzte Verfügbarkeit und Integrität sicherzustellen.
11205	Die Organisation verpflichtet sich, Geräte, Betriebsmittel, Information oder Software nicht ohne vorherige Genehmigung vom Betriebsgelände zu entfernen.
11206	Die Organisation verpflichtet sich, dass Werte außerhalb des Standorts gesichert werden, um die verschiedenen Risiken beim Betrieb außerhalb der Räumlichkeiten der Organisation zu berücksichtigen.
11207	Die Organisation verpflichtet sich, dass alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.
11208	Die Organisation verpflichtet sich, dass die Benutzer sicherstellen, dass unbeaufsichtigte Geräte und Betriebsmittel angemessen geschützt werden.
11209	Die Organisation verpflichtet sich, Richtlinien für eine aufgeräumte Arbeitsumgebung (Clean-Desk) hinsichtlich Unterlagen und Wechseldatenträgern und für Bildschirmsperren (Clear-Screen) für informationsverarbeitende Einrichtungen anzuwenden.

11310	Die Organisation verpflichtet sich, die Bedienabläufe zu dokumentieren und allen Benutzern, die sie benötigen, zugänglich zu machen.
11311	Die Organisation verpflichtet sich, dass Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und an den Systemen gesteuert werden.
11312	Die Organisation verpflichtet sich, die Ressourcennutzung/Benutzung von Ressourcen zu überwachen und abzustimmen, und es werden Prognosen zu zukünftigen Kapazitätsanforderungen erstellt, um die erforderliche Systemleistung sicherzustellen.
11313	Die Organisation verpflichtet sich, Entwicklungs-, Test- und Betriebsumgebungen voneinander zu trennen, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.
11314	Die Organisation verpflichtet sich, Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer umzusetzen.
11315	Die Organisation verpflichtet sich, Sicherheitskopien von Information, Software und Systemabbildern entsprechend einer vereinbarten Sicherungsrichtlinie anzufertigen und regelmäßig zu testen.
11316	Die Organisation verpflichtet sich, Ereignisprotokolle, die Benutzertätigkeiten, Ausnahmen, Störungen und Informationssicherheitsvorfälle aufzeichnen, zu erzeugen, aufzubewahren und regelmäßig zu überprüfen.
11317	Die Organisation verpflichtet sich, Protokollierungseinrichtungen und Protokollinformation vor Manipulation und unbefugtem Zugriff zu schützen.
11318	Die Organisation verpflichtet sich, dass die Uhren aller relevanten informationsverarbeitenden Systeme innerhalb einer Organisation oder einem Sicherheitsbereich mit einer einzigen Referenzzeitquelle synchronisiert werden.
11319	Die Organisation verpflichtet sich, für eine sichere Infrastruktur wie: Firewall, AV, Patch, MDM, Crypt HDD für mobile Endgeräte, 3-Wege Backup der Daten, Abgeschlossener Serverraum, Sichere Passwörter der Mitarbeiter-Accounts, MFA für alle Systeme mit Kundendatenbezug ==> zu viele Datenschutzüberschneidungen
11401	Die Organisation verpflichtet sich, Netzwerke zu steuern und zu verwalten, um Information in Systemen und Anwendungen zu schützen
11402	Die Organisation verpflichtet sich, Sicherheitsmechanismen, Dienstgüte und Anforderungen an die Verwaltung aller Netzwerkdienste zu bestimmen und sowohl für interne als auch für ausgegliederte Netzwerkdienste in Vereinbarungen aufzunehmen.

11403	Die Organisation verpflichtet sich, Vereinbarungen zu treffen, zur sicheren Übertragung von Geschäftsinformation zwischen der Organisation und externen Parteien.
11404	Die Organisation verpflichtet sich, dass Information in der elektronischen Nachrichtenübermittlung angemessen geschützt sind.
11405	Die Organisation verpflichtet sich, dass die Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, zu identifizieren, regelmäßig zu überprüfen und zu dokumentieren.
11501	Die Organisation verpflichtet sich, die Testdaten des Kunden sorgfältig zu schützen.
11601	Die Organisation verpflichtet sich, dass die Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation mit dem Zulieferer vereinbart und dokumentiert werden.
11602	Die Organisation verpflichtet sich, die Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, in Vereinbarungen mit Lieferanten aufgenommen werden.
11603	Die Organisation verpflichtet sich, den Lieferanten regelmäßig (z.B. alle 2 Jahre) zu überprüfen.
11701	Die Organisation verpflichtet sich, Aufzeichnungen gemäß gesetzlichen, regulatorischen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung zu schützen.
11702	Die Organisation verpflichtet sich, die Privatsphäre und der Schutz von personenbezogener Information, soweit anwendbar, entsprechend den Anforderungen der relevanten Gesetze und Vorschriften sicherzustellen.

_____, _____
Ort Datum

_____
Stempel, Unterschrift Organisation