Allgemeine Grundsätze und Geltungsbereich

Diese Richtlinie dient der Klassifizierung der Informationen, welche in der Schönek Gruppe und ihren Partnern für die Erfüllung der verschiedenen Aufgaben benötigt werden.

Diese Richtlinie gilt für alle Mitarbeiter der Schönek Gruppe und all ihren Partnern.

1) Die Erstellung dieser Richtlinie ist Teil der Implementierung des Informationsmanagementsystems nach VDA, wie im Managementreview des Geschäftsjahres 2021 festgelegt.

2) Informationen können in unterschiedlicher Form und auf unterschiedlichen Medien zur Verfügung stehen, wie z.B.:

- elektronisch (z.B. Partnersysteme, Kundeninformationen, Bestandsdaten, E-Mails, Internet)
- auf Datenträgern (z.B. Disketten, Festplatten, CDs, DVDs, USB-Sticks, Chipkarten)
- in Papierform (z.B. Schriftstücke, Dokumente, Fax-Ausdrucke, Zeichnungen, Veröffentlichungen)
- als Sprache (z.B. Besprechungen, Telefongespräche, Mitteilungen, Sprachaufzeichnungen, Vorträge)
- visuell (z.B. als Bild)

3) Die Informationen in der Schönek Gruppe sind angemessen, wirksam und durchgängig vor den jeweils identifizierten Bedrohungen zu schützen. Die Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit müssen in einer angemessenen und wirtschaftlich sinnvollen Weise gewährleistet werden. In Projekten ist nach Erreichen bestimmter Meilensteine zu prüfen, ob sich die Art der Information geändert hat und die Schutzziele angepasst werden müssen. Bei Kundenprojekten gelten zusätzlich die in den Lastenheften und mitgeltenden Unterlagen beschrieben Anforderungen zur Informationssicherheit.

4) Die folgenden Fragen können bei der Klassifizierung eigener Informationen unterstützen und die Zuordnung zu den Klassifizierungsstufen erleichtern:

- Welche Auswirkungen gäbe es wenn die Informationen in die Hände von Mitbewerbern gelangen? Wie hoch wäre dieser Schaden einzuschätzen?
- Welcher Schaden für die Schönek Geschäftsfelder wäre möglich, wenn die betroffenen Information in „falsche Hände“ geraten oder zerstört werden? Wie hoch wäre dieser Schaden einzuschätzen?
- Wäre der unbeabsichtigte Verlust oder die Zerstörung dieser Informationen mit hohen Kosten für den die Schönek Gruppe und deren Partnern verbunden?
- Könnte die Veröffentlichung dieser Informationen zu Rechtsverstößen, anderen rechtlichen Konsequenzen oder der Verletzung von sonstigen regulatorischen oder vertraglichen Verpflichtungen führen?
- Könnte der Missbrauch oder die Veröffentlichung dieser Informationen zu Ermittlungshandlungen durch Behörden führen?
- Welche Auswirkungen hätte unbeabsichtigter Verlust oder Zerstörung dieser Informationen auf die Motivation der Schönek Angestellten?
- Ist die Information bei Zerstörung oder Verlust wiederherstellbar und welcher Aufwand (Zeit und Geld) ist dafür notwendig?

Klassifizierung nach Vertraulichkeit

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele
Stufe 1: Öffentlich	Öffentliche Informationswerte sind für eine Verbreitung oder Nutzung im öffentlichen (z.B. Presse) oder virtuellen Raum (Internet allgemein, z.B. Foren, facebook etc.) vorgesehen und von dazu bestimmten Stellen der Schönek Gruppe zugelassen. Öffentliche Informationen stellen bei ihrer Verbreitung oder Nutzung im öffentlichen (z.B. Presse) oder virtuellen Raum (Internet allgemein, z.B. Foren, facebook etc.) kein Risiko für Schönek dar.	Besondere Schutzmaßnahmen sind nicht erforderlich. Werden Informationsgüter als „öffentlich“ dokumentiert, muss sichergestellt sein, dass keine Informationen höherer Sicherheitsstufen preisgegeben werden können. Öffentlich eingestufte Informationen sind vor ihrer Verbreitung oder Veröffentlichung mit der Geschäftsleitung oder deren Vertretern abzustimmen. Die Kennzeichnung hat mit dem Schriftzug "öffentlich“ zu erfolgen.	- Werbefilme - Produktbeschreibungen - Inhalte des Internetauftritts - Werbefotos - Pressemitteilungen - Publikationen in Zeitschriften und Büchern - Image Broschüren - Präsentationen auf öffentlichen Kongressen
Sicherheitsstufe	**Bedeutung**	**Behandlung**	**Beispiele**

Stufe 2: Intern	Interne Informationen sind nur für Schönek Gruppe Mitarbeiter vorgesehen, jedoch nicht für die Öffentlichkeit bestimmt. „Interne“ Informationen haben bei Offenlegung oder unberechtigte Kenntnisnahme begrenzte negative Auswirkungen auf die Schönek Gruppe. „Intern“ ist die Standard-Sicherheitsstufe für alle Informationen in der Schönek Gruppe, die nicht anders eingestuft bzw. gekennzeichnet sind.	Es ist sicher zu stellen, dass keine unberechtigte Person Zugriff auf die Informationen bekommt. Dies gilt für die Verarbeitung, Speicherung / Aufbewahrung, den Transport / Versandt und die Entsorgung / Vernichtung. Für externe Dienstleister ist die Unterzeichnung einer gesonderten Vertraulichkeitserklärung erforderlich, bevor Zugang auf „Interne“ Informationen gewährt werden kann. Eine Kennzeichnung ist nicht zwingend erforderlich, sollte jedoch falls gefordert mit dem Schriftzug „Intern“ erfolgen.	- Inhalte des internen Servers - Firmenrichtlinien und -anweisungen - Interne informelle Präsentationen - Informationen für Mitarbeiter - Betriebsvereinbarungen

Sicherheitsstufe	**Bedeutung**	**Behandlung**	**Beispiele**
Stufe 3: Vertraulich	Vertrauliche Informationen sind nur für eine eingeschränkte Gruppe von Personen vorgesehen und nicht für die Öffentlichkeit bestimmt. „Vertrauliche“ Informationen haben bei Offenlegung oder unberechtigte Kenntnisnahme erhebliche negative Auswirkungen auf das Unternehmen (z.B. finanziell, im Wettbewerb oder bei der Rechtslage).	Es ist sicher zu stellen, das eine Einsichtnahme in oder Zugriff auf diese Informationswerte nur durch einen vom Informationseigner legitimierten Personenkreis erfolgen kann. Für externe Dienstleister ist die Unterzeichnung einer gesonderten Vertraulichkeitserklärung erforderlich, bevor Zugang auf vertrauliche Informationen gewährt werden kann. Personenbezogene Daten sind grundsätzlich als vertraulich zu klassifizieren.	- Privatanschrift - Gehaltsinformationen - Geschäftsberichte - Informationen aus der Entwicklung - Daten der internen Finanzbuchhaltung - Audit Berichte - Kundenanforderung aus Lastenheften in Verbindung mit den gelten Bestimmungen zur Informationssicherheit

Stufe 4: Streng vertraulich	Streng vertrauliche Informationen sind nur für einzelne benannte Personen vorgesehen. „Streng vertrauliche“ Informationen haben bei Offenlegung oder unberechtigte Kenntnisnahme schwerste negative Auswirkungen auf die Schönek Gruppe, Geschäftspartner oder Mitarbeiter. (z.B. ist die Existenz eines oder mehrerer Schönek Gruppe Bereiche gefährdet oder es sind erhebliche rechtliche Konsequenzen für Schönek zu erwarten.)	Streng vertrauliche Informationen / Daten, dürfen nur dem vom Eigentümer der Informationen im Einzelfall bestimmten namentlich benannten Personen zugänglich gemacht werden. Vor der Weitergabe muss sichergestellt werden, dass die Identität des Empfängers belegbar geprüft wurde. Die Entscheidung zur Weitergabe oder Weiterverarbeitung trifft der Informationseigentümer für jeden Einzelfall.	- Unternehmensgeschäftsberichte vor Veröffentlichung - Geschäftsgeheimnisse - Insiderinformationen - kundenspezifische Baugruppenzeichnung

Klassifizierung nach Integrität

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele
Stufe 1: Ungesicherte Integrität	Informationen / Daten ungesicherter Integrität sind Informationen, die nur einmalig verwendet werden oder deren Wiederherstellung ohne Aufwand möglich ist. Eine unautorisierte Veränderung hat keine Auswirkungen auf den Geschäftsbetrieb der Schönek Gruppe.	Für Informationen / Daten der Einstufung „Ungesicherte Integrität“ sind keine besonderen Maßnahmen zur Wahrung der Integrität oder Verbindlichkeit vorzusehen.	Kopien öffentlicher Informationen

Stufe 2: Gesicherte Integrität	Informationen / Daten gesicherter Integrität sind Informationen, die mehrfach verwendet werden oder deren Wiederherstellung bei unautorisierter Veränderung mit mittlerem Aufwand möglich ist. Eine unautorisierte Veränderung der Informationen / Daten hat begrenzte negative Auswirkungen auf die Schönek Gruppe. „Gesicherte Integrität“ ist die Standard- Sicherheitsstufe für alle Informationen in der Schönek Gruppe, die nicht anders eingestuft bzw. gekennzeichnet sind.	Informationen / Daten der Einstufung „Gesicherte Integrität“ müssen Vorkehrungen zum Schutz gegen Veränderungen durch Unbefugte aufweisen. Dies gilt für die Verarbeitung, Speicherung / Aufbewahrung und den Transport / Versandt. Die Sicherstellung der Integrität und Verbindlichkeit erfolgt in dieser Stufe in der Regel durch die eingesetzten Systeme bzw. Anwendungen. Veränderungen sind auf einen definierten Kreis von Personen beschränkt.	- Projektarbeitsdateien - Besprechungsprotokolle
Sicherheitsstufe	**Bedeutung**	**Behandlung**	**Beispiele**
Stufe 3: Prüfbare Integrität	Informationen / Daten prüfbarer Integrität sind Informationen, die vielfach verwendet werden oder deren Wiederherstellung bei unautorisierter Veränderung nur mit sehr hohem Aufwand möglich ist. Eine unautorisierte Veränderung der Informationen/ Daten hat erhebliche negative Auswirkungen auf die Schönek Gruppe (z.B. Finanziell, im Wettbewerb oder bei der Rechtslage).	Informationen / Daten der Einstufung „Prüfbare Integrität“ müssen Vorkehrungen zum Schutz gegen Veränderungen durch Unbefugte aufweisen. Informationen / Daten der Einstufung „Prüfbare Integrität“ müssen eine Möglichkeit bieten, Verletzungen der Integrität festzustellen. Die Verbindlichkeit wird über die prüfbare Dokumentation einer eindeutigen Kennung sichergestellt. Veränderungen sind nachvollziehbar dokumentiert und nur durch einen eingeschränkten autorisierten und eindeutig identifizierbaren Personenkreis möglich.	- Arbeitsanweisungen - Prüfberichte - Sicherheitsanweisungen - Produktbeschreibungen - Inhalte des Internetauftritts - Pressemitteilungen - Image Broschüren - E-Mails

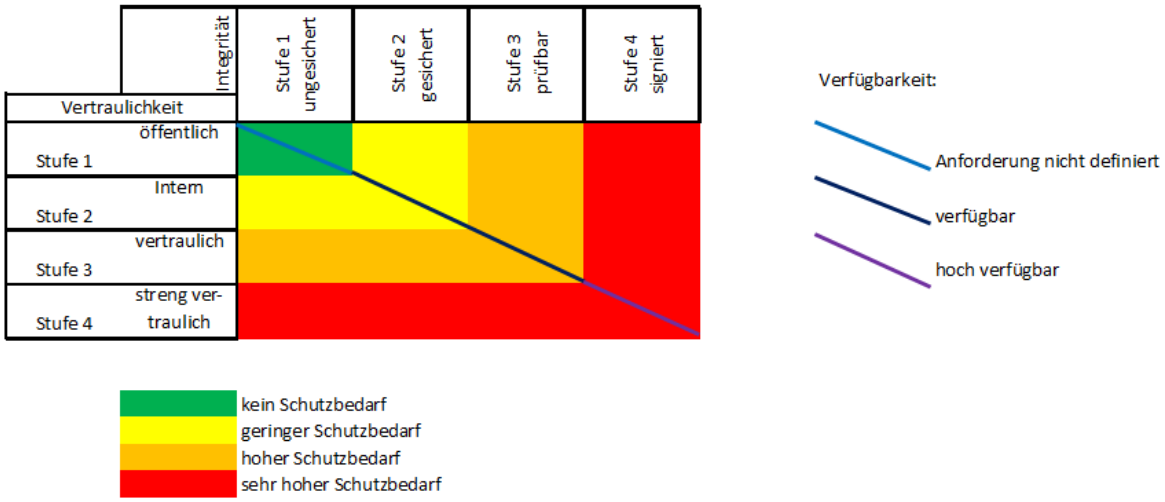
Stufe 4: Signierte Integrität	Informationen / Daten signierter Integrität sind Informationen, die vielfach verwendet werden oder deren Wiederherstellung bei unautorisierter Veränderung nicht mehr möglich ist.	Für solche Informationen / Daten müssen besondere Schutzvorkehrungen gegen Veränderungen durch Unbefugte getroffen werden. Die Informationen / Daten müssen mit einer personen- oder systembeziehbaren Signatur zur Integritätsprüfung versehen werden.	- Firmenrichtlinien - Firmenanweisungen - Betriebsvereinbarungen - Geschäftsberichte - Bilanzen - Dokumentierte Entwicklungsstände
Sicherheitsstufe	**Bedeutung**	**Behandlung**	**Beispiele**
Stufe 4: Signierte Integrität	Eine unautorisierte Veränderung der Informationen / Daten hat erhebliche schwerste negative Auswirkungen auf die Schönek Gruppe, Geschäftspartner oder Mitarbeiter (z.B. ist die Existenz eines oder mehrerer Bereiche gefährdet oder es sind erhebliche rechtliche Konsequenzen für Schönek zu erwarten.)	Ersteller, Prüfer, Freigebende, Absender und der Eigentümer der Informationen muss gesichert dokumentiert werden. Jede Veränderung muss nach einem dokumentierten gesicherten Verfahren nachvollziehbar und prüfbar sein und darf nur den namentlich benannten und eineindeutig identifizierbaren Personen möglich sein.	

Klassifizierung nach Verfügbarkeit

Sicherheitsstufe	**Bedeutung**	**Behandlung**	**Beispiele**
Stufe 1: Anforderung nicht definiert	Eine Nicht-Verfügbarkeit der Informationen hat keine Auswirkungen auf den Geschäftsbetrieb der Schönek Gruppe.	Informationen / Daten, IT Systeme und IT Dienste der Stufe 1 unterliegen keinen besonderen Anforderungen an die Verfügbarkeit. Die Verfahren richten sich nach der sinnvollen und wirtschaftlichen angemessenen Realisierung von Maßnahmen und Abläufen.	- Offlinedaten aus dem Internet - Arbeitskopien

Stufe 2:Verfügbar	Eine Nicht-Verfügbarkeit der Informationen hat Auswirkungen auf den Geschäftsbetrieb der Schönek Gruppe, jedoch nicht die Existenz gefährdend und nur begrenzte negative Auswirkungen auf die Schönek Gruppe.„Verfügbar“ ist die Standard-Verfügbarkeitsstufe für alle Informationen, IT Systeme und ITDienste der Schönek Gruppe, die nicht anders eingestuft bzw. gekennzeichnet sind.	Informationen / Daten, IT Systeme und IT Dienste, die als „Verfügbar“ eingestuft werden, müssen sich innerhalb eines fest definierten Zeitraums wiederherstellen oder ersetzen lassen.Es muss ein Wiederherstellungskonzept vorhanden sein, das bei Ausfall der IT sicherstellt, dass Funktionen und Informationen nach der fest definierten Zeitspanne wieder zur Verfügung stehen.Das Verfügbarkeitskonzept ist zu dokumentieren.	- Internetauftritt - Firmenrichtlinien - Firmenanweisungen - Publikationen - Zeitaufwendige Präsentationen - Entwicklungsunterlagen - IT Systeme, z.B. Server
Stufe 3: Hoch verfügbar	Eine Nicht-Verfügbarkeit der Informationen hat schwere negative Auswirkungen auf die Schönek Gruppe, Geschäftspartner oder Mitarbeiter. (z.B. ist die Existenz der Schönek Gruppe oder einer ihrer Partner gefährdet, es sind erhebliche rechtliche Konsequenzen für die Schönek Gruppe zu erwarten.)	Es muss die Mindestverfügbarkeit von Informationen / Daten, IT Systeme und IT Diensten für den Normalfall und eine Mindestverfügbarkeit für den Notfall angegeben werden. Die Informationen sind redundant zu handhaben, sodass bei Ausfall und Zerstörung von Informationen und Systemen eine akzeptable Beeinträchtigung der Geschäftsprozesse entsteht. Das Verfügbarkeitskonzept ist detailliert zu dokumentieren und regelmäßig zu prüfen. Ein Notfall Konzept (Disaster Recovery) muss detailliert dokumentiert und regelmäßig getestet werden.	- Informationen der Produktionssteuerung - Finanzberichtserstattung

Einteilung des Schutzbedarfs (Farbdiagramm):



Für die Festlegung des Schutzbedarfs der Informationen bietet das Farbdiagramm eine Entscheidungshilfe.
Es gilt immer der höchste anzuwenden.
Schutzbedarf für die jeweilige Information, unabhängig von der sonstigen Aufteilung in den Punkten Vertraulichkeit, Integrität oder Verfügbarkeit.

Beispiel: Die Information ist streng vertraulich, prüfbar und verfügbar = sehr hoher Schutzbedarf

ACHTUNG:
Sollte nicht eindeutig klar sein, zu welchem Schutzbedarf die Ihnen vorliegende Information gehört,
-so ist bei Dokumenten zu Projektthemen immer von der Klassifizierung **"sehr hoher Schutzbedarf"** auszugehen!
- und bei allen anderen Dokumente immer mindestens von der Klassifizierung "geringer Schutzbedarf"!
Unbekannte Klassifikation einer Information verpflichtet vor externem Versand zur definierten Einstufung durch den Urheber oder Technischen Leiter.