Zielsetzung des Arbeitskreises Informationssicherheit– Fachausschuss Instandhaltung

AK Informationssicherheit Rubrik A2	
Obmann/Obfrau	Paul Sander (Teut Betriebsführung)
AK eingesetzt vom FAIH am	28.02.2022
Zielsetzung bestätigt am	28.02.2022
Wann will der AK das Ergebnis vorstellen?	Veröffentlichung der Rubrik XX für Q1/2023 geplant
Was ist die Problemstellung, was gehört inhaltlich dazu?	Die BSI-KritisV ist seit 1.1.2022 in Kraft, wodurch viele Betreiber von Erzeugungsanlagen (EZA) und virtuellen Kraftwerken (Anlagen zur Bündelung/ Steuerung elektrischer Leistung) verantwortlich für die Umsetzung von technischen und organisatorischen Maßnahmen für Kritische Infrastrukturen sind. Die Schwellenwerte liegen bei 104 MW installierte Nettoleistung (bzw. 36 MW bei Regelleistung). Da in der Windenergiebranche unterschiedliche Unternehmensmodelle mit verschiedenen Akteuren und kleinteiligen Eigentümerstrukturen kooperieren, ist es zum jetzigen Zeitpunkt nicht abschließend geklärt, in welchem Umfang bestimmte Marktteilnehmende von den Anforderungen des BSIG und EnWG betroffen sind: - Wer muss ein Managementsystem für Informationssicherheit (ISMS) implementieren? - Wo liegen die Grenzen des ISMS (Geltungsbereich)? - Welche Akteure besitzen schreibenden oder lediglich lesenden Zugriff auf Teile der IT-Infrastruktur? - Welche Datenschnittstellen sind von welchen Maßnahmen betroffen? - Welche Datenübermittlungsverfahren sind von welchen Maßnahmen betroffen?
Was ist das Ziel, welches Ergebnis möchte der AK erarbeiten?	Klarstellung der erforderlichen IT-Sicherheitsmaßnahmen für die Windenergiebranche zur Erfüllung des geforderten gesetzlichen und normativen Rahmens
Soll die Unterlage als Empfehlung, Prüfvorschrift oder Zertifizierungsvorschrift erstellt werden?	Als Empfehlung an Akteure, vor allem Betreiber und Betriebsführer der Windenergiebranche

Was (Listen, Darstellungen, Erklärungen, Empfehlungen) soll die Richtlinie, der Teil oder die Rubrik am Ende konkret enthalten?	- Darstellung der Mindestanforderungen für betroffene Akteure (Kriterienkatalog, Checkliste) unter Betrachtung von Beispielen kleiner Parkstrukturen mit unterschiedlichen Verantwortungs-/ Betriebsmodellen (Outsourcing in den unterschiedlichen Aufgaben ja/nein).
	- Darstellung und Definition der Datenschnittstellen
	- Lieferantenbeziehungen: Welche Lieferanten haben Zugriff auf welche Systeme?
	- Lieferantenmanagement: Festlegen eines Klassifizierungsschema
	- Beispielhafte Ausgestaltung der zu treffenden Maßnahmen nach Anforderungen der DIN/ISO/IEC 27000er Reihe
	  ○ Aufzählung der Bestandteile eines ISMS unter Beachtung des Top Down Prinzips. Dabei sollen nicht alle Anwendungsfälle konkret ausgestaltet werden, sondern lediglich Hinweise auf Probleme und Fallstricke gebracht werden.
	  ○ Beschreibung der Möglichkeiten der Implementation von ISMS bei verschiedenen Konstellationen der Verantwortung und Organisation der Akteure/ Unternehmen in EZA (unterschiedliche Grade von Outsourcing). Beschreibung der Anforderungen unter Beachtung der vertraglichen Absicherung und des gesetzten Anwendungsbereichs.

Wie häufig will sich der AK treffen?	Alle 2 Monate 2-stündige Web-Meetings
Welche Recherchen bzgl. des bestehenden Regelwerks z.B. zum Zweck der Abgrenzung oder für Klarstellungen sind nötig?	BSI-KritisV, B3S Aggregatoren, EnWG, BSIG, IT-Sicherheitsgesetz, ISO/IEC-27000-Reihe, BWE IT-Orientierungshilfe Wind, etc.
Gegen welche bestehende Normung muss sich der AK bzw. das Ergebnis abgrenzen?	Siehe oben
Was soll explizit nicht behandelt werden?	Darstellung des rechtlichen Rahmens (Inhalt „IT-Orientierungshilfe Wind“ des BWE)

Welche Experten- oder Interessenkreise sind bereits beteiligt?	Betreiber, Betriebsführer, Hersteller, Dienstleister (z.B. CMS)
Welche Experten- oder Interessenkreise müssen zusätzlich eingebunden werden?	Netzbetreiber, Direktvermarkter