Belehrung Informationssicherheit für externe Dienstleister

Inhaltsverzeichnis

1. Zielstellung

Die Anlagensteuerung und -überwachung für den Gasspeicherbetrieb UGS Bernburg und UGS Bad Lauchstädt erfordert die tägliche Nutzung von Informations- und Kommunikationstechnologie (IKT) zur Erfassung, Aus- und Bewertung von Daten und dem daraus resultierenden Steuerungsbedarf. Um diese Kernaufgabe der VNG Gasspeicher GmbH (VGS) störungsfrei und zuverlässig zu erfüllen ist die sichere und korrekte Handhabung dieser kritischen Systeme, Geräte und Daten sowie deren Schutz zwingend notwendig. Dies geschieht regelmäßig auch unter Einbeziehung externer Dienstleister.

Diese Belehrung informiert Sie, als Mitarbeiter eines externen Unternehmens, über die grundlegenden Regelungen im Umgang mit der vor Ort befindlichen IKT und, wie mit den erzeugten bzw. genutzten Daten und Dokumenten zu verfahren ist. Die Einhaltung dieser Vorgaben ist ein wesentlicher Baustein für den sicheren Anlagenbetrieb der Kritischen Infrastruktur der VGS.

2. Geltungsbereich

Diese Belehrung gilt für alle Beschäftigten von Firmen, welche durch die VGS beauftragt wurden, Arbeiten an den Standorten UGS Bernburg bzw. UGS Bad Lauchstädt durchzuführen, die im Zusammenhang mit Informations- und Kommunikationstechnologie der Kritischen Infrastruktur dieser beiden Standorte stehen.

Die Verpflichtung zur Einhaltung der hier getroffenen Regelungen ergibt sich aus dem entsprechenden Dienstleistungsvertrag.

Über Änderungen und Ergänzungen zu den bestehenden Regeln und Dokumenten wird in geeigneter Form informiert.

3. Organisation der Informationssicherheit

Zuständig für alle die Informationssicherheit betreffenden Themen ist der durch die Geschäftsführung bestellte Informationssicherheitsbeauftragte (ISB).

Im Rahmen Ihrer Tätigkeit wird Ihnen ein Mitarbeiter der VGS aus dem entsprechenden Bereich als Ansprechpartner benannt. Sofern Ihnen Unregelmäßigkeiten auffallen, welche die Informationssicherheit betreffen oder betreffen könnten teilen Sie Ihre Beobachtung dem Mitarbeiter mit. Dieser übernimmt die weitere betriebsinterne Kommunikation.

4. Grundregeln im Umgang mit IKT und Daten

Für die Erledigung Ihrer Arbeit stellt Ihnen die VGS bei Bedarf entsprechende Systeme, Geräte und Anwendungen für die Arbeit an der Automatisierungs- und Fernwirktechnik sowie für die Verarbeitung von Daten zur Verfügung. Sofern Ihr Auftrag dies erfordert ist der Einsatz von Geräten Ihrer Firma im Rahmen der hier definierten Vorgaben möglich.

Im Umgang mit sämtlichen Geräten / Anwendungen / Daten der Kritischen Infrastruktur gelten die folgenden allgemeinen Grundsätze:

- Bewegen Sie sich ausschließlich in Bereichen, die für die Ausübung Ihrer Tätigkeit relevant sind.

- Sie haben zu jeder Zeit die Vorgaben des Personals der VGS zu befolgen.

- Sofern Sie externe Geräte bzw. Datenspeicher zur Ausübung Ihrer Tätigkeit an IKT der VGS anschließen müssen darf dies erst nach der Freigabe durch die VGS erfolgen.

- Sicherungseinstellungen, -systeme oder sonstige Vorkehrungen zum Schutz der IKT dürfen nicht außer Betrieb genommen, umgangen oder in sonstiger Weise verändert werden. Sofern Ihre Arbeit eine der beschriebenen Maßnahmen erfordert darf dies nur mit entsprechender Genehmigung durch die VGS erfolgen.

- Sämtliche Informationen über Art und Aufbau der IKT sind vertraulich zu behandeln und dürfen nur an Personen Ihrer Firma weitergegeben werden, sofern dies notwendig ist, um die vereinbarten Leistungen zu erbringen. Eine Weitergabe darüber hinaus, insbesondere an Dritte, hat in jedem Fall zu unterbleiben.

- Sämtliche Informationen, die im Zusammenhang mit dem Zugriff auf IKT der VGS erhalten werden oder zugänglich sind, müssen streng vertraulich behandelt werden. Die Informationen sind nur für den bestimmungsmäßigen Gebrauch zu verwenden und insbesondere nicht an Dritte weiterzugeben.

- Die Mitnahme von Dokumenten, Daten, Arbeitsergebnissen oder IKT-Systemen außerhalb der Geschäftsräume der VGS ist grundsätzlich nicht gestattet. Ausnahmen bedürfen der vorherigen schriftlichen Genehmigung durch die entsprechend zuständigen Bereichsleiter.

5. Detaillierte Regelungen

In den nachfolgenden Abschnitten werden konkrete Regeln und Handlungsanweisungen aufgeführt.

5.1. Umgang mit Passwörtern

Sofern Sie ein Passwort zur Anmeldung an Systemen der VGS erhalten, gilt es folgende Punkte einzuhalten:

- Das Passwort ist nur und ausschließlich von Ihnen zu nutzen.

- Eine Weitergabe an Dritte, als auch Mitarbeiter Ihrer Firma ist nicht gestattet.

- Sofern das Passwort Dritten bekannt geworden sein sollte, ist dies umgehend dem zuständigen Mitarbeiter der VGS zu melden.

5.2. Zugangs- und Zugriffsschutz

Berechtigungen regeln den Zugriff auf Daten und werden technisch sichergestellt. Sofern Sie erkennen, dass Sie fehlerhaft eine Berechtigung erhalten haben, sind Sie nicht berechtigt, von dieser Berechtigung Gebrauch zu machen. Teilen Sie den Fehler umgehend dem jeweiligen Systemverantwortlichen mit.

Versuchen Sie nicht, Zugriff auf Daten zu bekommen, zu denen Sie keine Zugriffsberechtigung haben.

5.3. Umgang mit Hardware

Es sind alle Geräte innerhalb der Büro- und Betriebsräume, als auch auf dem Betriebsgelände, mit Sorgfalt zu behandeln. Die Geräte sind nur für den dafür vorgesehen Gebrauch zu verwenden. Eine davon abweichende Nutzung ist untersagt. Die Nutzung von Geräten ist mit dem zuständigen Ansprechpartner bei der VGS vorab abzustimmen.

Schützen Sie die Geräte vor Beschädigungen durch Umwelteinflüsse wie Hitze, Kälte und Wasser und bei Stürzen.

Sofern Ihnen Geräte direkt zugeteilt wurden, sind Sie stets für diese verantwortlich. Eine Übertragung dieser Verantwortung an Kollegen ist nur mit Genehmigung der VGS möglich und muss schriftlich dokumentiert werden.

Der Verlust von Geräten ist umgehend dem zuständigen Ansprechpartner bei der VGS sowie dem zuständigen IT-Support (z.B. Service-Desk) zu melden.

5.4. Umgang mit Software

Sofern die Installation von Software auf IKT der VGS notwendig ist, darf dies nur nach Genehmigung durch den zuständigen Bereichsleiter erfolgen. Eine Begründung der Notwendigkeit sowie die Art und Funktion der Software sind zu dokumentieren. Nach Abschluss der Arbeiten muss die Software vollständig von der IKT der VGS entfernt werden, sofern diese nicht dauerhaft eingesetzt werden soll.

5.5. Nutzung des Internets

Sofern Ihnen für die Erledigung Ihrer Arbeit der Zugriff zum Internet aus dem Netz der VGS gewährt wird, hat die Nutzung ausschließlich hierfür zu erfolgen. Jegliche Nutzung darüber hinaus ist nicht gestattet.

5.6. Meldung von Informationssicherheitsvorfällen

Fallen Ihnen sicherheitsrelevante Vorgänge, Fehlverhalten oder Schwachstellen auf – z.B. solche, die durch diese Belehrung beschrieben werden – melden Sie diese umgehend Ihrem Ansprechpartner der VGS oder dem Informationssicherheitsbeauftragten der VGS (Email: informationssicherheit@vng-gasspeicher.de, Tel. 0341/443-2316).

5.7. Fehlhandlungen

Die Mitarbeiter der VGS und alle anderen Personen, die mit Informationen der VGS arbeiten, sind dazu verpflichtet, sich nicht von persönlicher Einflussnahme Dritter in Form von Einschüchterung, Überredung, Einschmeichelung oder nicht notwendiger Hilfeleistung zu Fehlhandlungen verleiten zu lassen.

Ausgenommen sind Handlungen Dritter, die die körperliche Unversehrtheit der jeweiligen Person oder Ihres privaten Umfeldes gefährden oder gefährden könnten.

Sofern Sie in eine solche Situation der Einflussnahme geraten, unterrichten Sie schnellstmöglich einen zuständigen Verantwortlichen der VGS, damit eine geeignete Lösung gefunden werden kann.

6. Maßnahmen nach Beendigung des Vertragsverhältnisses

Nach Abschluss Ihrer Arbeit sind die folgenden Punkte zu prüfen und gegebenenfalls umzusetzen:

- Dokumente und Daten sind dem Personal der VGS zu übergeben. Sofern eine Übergabe nicht möglich ist, sind die Dokumente und Daten nach Aufforderung zu vernichten bzw. so zu löschen, dass diese nicht wiederhergestellt werden können.

- Die erlangten Informationen über Standorte, Aufbau und Betrieb der IKT sowie Geschäftsdaten der VGS sind über das Ende des Vertragsverhältnis hinaus gemäß der Vertraulichkeitsvereinbarung als vertraulich zu behandeln.

- Sämtliche überlassene Hardware, Schlüssel, Ausweise, etc. sind abzugeben.