So handeln Sie bei einem IT-Sicherheitsvorfall richtig!

Fall 1

Bei einer **Datenpanne**, also in allen Fällen, in denen Personen unrechtmäßigen Zugang zu BLSV-Daten erhalten haben, beispielsweise bei versehentlich falschem Verteiler oder falschen Anhängen bei einem E-Mail-Versand, gilt:

1. Details zum Ereignis notieren nach dem Schema „Wann? Wer? Was?“.
2. Compliance informieren; diese informiert dann die Datenschutzbeauftragte.

   → compliance@blsv.de oder Tel. 089 15702 201
3. Vorgesetzte/n informieren; diese/r informiert dann GL oder GF.
4. Rückmeldung der Compliance abwarten zum weiteren Vorgehen.

Fall 2

Falls ein **illegaler Zugriff** auf ein BLSV-Gerät bemerkt oder auch nur vermutet wird, beispielsweise nach einem Cyber-Einbruch („Hacking“ oder „Phishing“), gilt:

1. Gerät isolieren, also Netzwerk/LAN-Kabel abziehen und WLAN deaktivieren. Gerät aber nicht ausschalten oder neu starten.
2. Details zum Ereignis notieren nach dem Schema „Wann? Wer? Was?“.
3. IT informieren (nur die IT unternimmt weitere technische Schritte!)

   → it@blsv.de oder Tel. 089 15702 343
4. Compliance informieren; diese informiert dann die Datenschutzbeauftragte.

   → compliance@blsv.de oder Tel. 089 15702 201
5. Vorgesetzte/n informieren; diese/r informiert dann GL oder GF.
6. Rückmeldung abwarten zum weiteren Vorgehen.

Sowohl aus technischen als auch aus datenschutzrechtlichen Gründen ist in allen Fällen Eile geboten, also bitte schnellstmöglich reagieren!

Danke!