Scottish Environment Protection Agency
Buidheann Dìon Àrainneachd na h-Alba

Our Ref: 2434
13th May 2022

Richard Leonard MSP
Convenor
Public Audit Committee
Room T3.60
The Scottish Parliament
EDINBURGH
EH99 1SP

Sent via email to: publicaudit.committee@parliament.scot

Dear Mr Leonard

The 2020/21 audit of the Scottish Environment Protection Agency

Thank you for your letter dated 22nd April 2022 allowing SEPA the opportunity to give further information on our current back-up strategy following on from the oral evidence we gave at the Committee on the 17th March 2022.

Following the cyber-attack which caused significant disruption to SEPA's Information Systems (IS) infrastructure and services, we have procured specialist expert support and with their help have carried out a full review and developed a robust strategy which ensures our current security and back up posture is robust and will help protect against future cyber events.

We have worked extensively with expert external partners to ensure resilience around our backup and recovery capabilities. The safeguards we have implemented, are focussed on strengthening our overall systems, through an enhanced back up regime to ensure business continuity is maintained in the event of future data breaches and cyber-attacks.

We are confident the systems we have in place are robust and based on best practice from leading experts in this field. Our systems will be subject to ongoing reviews and testing to ensure we are well placed in the event of future cyber events and in the face of ever-changing external threats.

The National Cyber Security Centre (NCSC) guidance on best practice around back up strategy is the implementation of the 3-2-1 rule. This means that if a copy is compromised, at least one other copy is intact. This is particularly relevant to ransomware attacks such as the one that SEPA experienced during the recent cyber-attack. In annex 1 you will find details of our information systems and our current back up regimes which supports these systems. In addition, we have included how these back up regimes will be improved and further developed as we continue our recovery.

Cont'd……

Chairman
Bob Downes
Acting Chief Executive
Jo Green
www.sepa.org.uk

SEPA Corporate Office
Strathallan House
Castle Business Park
Stirling
FK9 4TZ
Customer enquiries: 03000 99 66 99

I hope this information contained in this letter gives you the confidence that SEPA's back up strategy is in line with best practice guidance. We are not providing technical details because doing so would compromise our security posture. Clearly, if further information is required we can provide this to the Committee confidentially.

If I can help in any further way please do not hesitate to contact me.

Yours sincerely

Jo Green
Acting Chief Executive

Annex 1 SEPA's Backup Regime

SEPA's Current Backup Regime

SEPA's IS systems and data currently reside in three platforms: Cloud storage in MS Azure for Flood Warning and Digital Licensing systems; Cloud storage in MS 365 for office business applications such as e-mail, Teams and Document storage and on-premise for financial and specialist systems such as Payroll, HR & Finance as well as Laboratory Information System data storage.

Backups are applied to each platform as follows:

Our two cloud tenancies are fully backed up on a regular, frequent schedule, offsite at more than two separate Microsoft datacentres using Microsoft's backup software. Furthermore all our tenancies are backed up on site by frequent, incremental backups and full backups taken on two separate differing time cycles.

Further to this, a final layer of backups are taken onsite, on devices that are physically detached from SEPA's network infrastructure once the backup is complete.

On top of this comprehensive backup programme, SEPA IS continue to take and retain ad-hoc backups to significant changes and upgrades.

SEPA's Future Backup Regime

Our expert contractors have produced a more detailed design for a new backup suite that goes further than the NCSC 3-2-1 rule, and follows the 3-2-1-1-0 rule. Work on building this backup suite is underway and will be complete in the next few months.