National Security Vetting Solution (NSVS) e-Form portal Security Operating Procedures

Purpose

This document constitutes the baseline Security Instructions for the NSVS eForm Intranet and Internet Portals.

Scope

These Security Instructions apply to the authorised users of the NSVS eForm Portals by Vetting Sponsors and Subjects for the sole purpose of National Security Vetting.

Security Classification

The highest security classification of data submitted via the eForm Portals is Official-Sensitive-Personal. Users have a responsibility to ensure that the protective marking of any data they originate on the Portals does not exceed Official-Sensitive-Personal.

Password Policy

User IDs and Passwords shall not be disclosed to other individuals. Passwords may be written down but they must be stored and protected as Official-Sensitive.

Users must be vigilant to malicious requests for Username and Password details and must not disclose them to anyone. **You will never be asked or sent an official email or web link asking to provide account login details and passwords.**

Sponsors must not share their Sponsor login details or password with any other person. If other security colleagues within your organisation require a NSVS eForm portal account then a separate account request must be submitted for them.

Use of the Portals

Users must only use their NSVS eForm portal account for the purpose for which it is provided.

Vetting applications must only be submitted when there is an actual and confirmed requirement for the Subject to hold a security clearance. Speculative vetting requests are not permitted.

Vetting applications that have been requested but that are no longer required must be cancelled by the Sponsor at the earliest opportunity using the NSVS e-Form portal.

Sponsors must not share their Sponsor ID with anyone unless requested to do so by a member of UKSV Enquiry Centre staff.

Sponsors must not complete the sections of the vetting application intended to be completed by the Subject. Exceptions can be made where the Subject is physically unable to complete the form for disability reasons. In this particular circumstance the Subject must be present to ensure that all information entered is correct.

Security

Sponsors/Subjects accessing the intranet portal via a corporate device connected to the RLI/PSN must do so in accordance with the local security policy for the relevant system.

Sponsors/Subjects accessing the internet portal from a personal device must be aware of their location and not do so in a public place, or where they can be easily overlooked.

Access to the internet portal from an untrusted internet connection such as internet café is not permitted.

The email address for the Vetting Subject and Sponsor must belong to the individual and not be a shared group mailbox.

Reporting of Security Incidents

If Sponsors/Subjects suspect there has been a security incident with respect to the NSVS Portals they should report it to the NSVS IT Security Officer (ITSO) via the UKSV Enquiry Centre.

Security incidents may include, but are not limited to: data being entered onto the system with a higher classification than Official-Sensitive-Personal, anomalies in data on the system, a Sponsor/Subject logging on using another users details, suspicious system behaviour that may be indicative of a virus infection etc.

Sponsors should note, and consider reminding the Subject of the vetting, that both the Sponsor and Subject have 63 working days to complete their respective parts of the vetting application. Failure to do so will result in the application being cancelled, with all previously entered data being deleted.

Sponsors must notify the UKSV Enquiry Centre should an individual they have previously cleared leave employment. This is so vetting records can be accurately maintained.

Operating outside these procedures may constitute a breach of security and/or HMG policy. In these circumstances, it may result in suspension of account. By accepting this agreement you are confirming you agree to these terms.

Contacts

https://www.gov.uk/guidance/united-kingdom-security-vetting-contact-us

Further security guidance for holders of multiple eForm portal accounts.

It is the responsibility of sponsors to ensure that clearance requests are initiated from the correct sponsor account. If a clearance is initiated from an incorrect sponsor account, this clearance and its associated case data may be visible to an organisation that, while part of the security community, is not entitled to view the specific clearance in question. This would be a breach of both the Data Protection Act and these e-Form portal security instructions on the part of the sponsor.