

CESG's Incident Response team (GovCertUK)

Guidance for Reporting an Incident

Introduction

One of CESG's roles is to minimize the risk and effects of electronic attack to the Government community. As CESG's Computer Emergency Response Team, GovCertUK assists Government departments and organisations in the recovery from a computer security incident. We gather data from all available sources to monitor the general threat level and focus. For these reasons the early reporting of incidents and attempted attacks is highly recommended.

To assist in the identification and categorisation of an event please read GovCertUK's [Incident Response Guidelines \(pdf\)](#) for further information and guidance.

Reporting Process

Incidents should be reported by the Departmental Security Officer, or equivalent (or an individual authorized by the DSO). All Incidents should be made to:

Telephone number **01242 709311** for an initial response, and should be followed up with an email to incidents@govcertuk.gov.uk using the [incident template \(doc\)](#).

Where possible as much supporting information as possible should be supplied, such as log files, internal/external IP addresses, affected Operating Systems, patch levels and policy etc.

How to submit malware samples to GovCertUK

All samples should be sent by carefully following the procedures below:

- 1.) All samples should be renamed to <originalfilename>.<originalfileextension>.txt.
- 2.) All samples should then be zipped and password protected with the password 'infected'.
- 3.) Optionally (but recommended), PGP encrypt the message (and attachments) to the GovCertUK Public Key, available <HERE>
- 4.) Use the following subject line: 'MALWARE SAMPLE'
- 5.) Send the message to samples@govcertuk.gov.uk

NB: Any classified samples from Government departments should be burnt to CD/DVD, appropriately labeled and sent to:

GovCertUK
A2f
CESG
P.O. Box 144
Cheltenham
Gloucestershire
GL51 0EX UK