

Cyber Security Preparedness IGT Administrator Guide

The Health and Social Care Information Centre (HSCIC) has been asked to take on an enhanced role by the Secretary of State for Health to help ensure data security across the care system. For further information see the HSCIC website at:

<http://www.hscic.gov.uk/datasecprop>

As part of this enhanced role, there is a requirement to gather information on organisations' Cyber Preparedness. Information gathering is mandated for NHS Acute, Ambulance, Community and Mental Health Trusts; Commissioning Support Units, and Accredited Safe Haven Clinical Commissioning Groups.


Your response will not impact on your Information Governance Toolkit Score.

The information gathering is in the form of a survey. The survey is a series of questions that are either scaled (Strongly Agree to Strongly Disagree) or have more factual yes/no responses.

Additional functionality has been added to the IG Toolkit to allow your Senior Information Risk Owner (SIRO) to complete the survey. Where your SIRO is already a registered IG Toolkit user, you should add the role of 'SIRO' to his/her account details. If the SIRO does not have an existing IG Toolkit account, you will need to create a new user account for him/her ensuring the SIRO role is ticked.

You are here: [Admin](#) > [Organisation Admin](#) > [Edit](#) > [User Admin](#) > [New User](#)

User Details Admin

User ID: (leave blank for default)	<input type="text"/>	Roles: <ul style="list-style-type: none"><input type="checkbox"/> Incidents Reporting User<input type="checkbox"/> Information Mapping Admin<input type="checkbox"/> Information Mapping User<input type="checkbox"/> Organisation Administrator<input type="checkbox"/> Organisation Auditor<input type="checkbox"/> Organisation Reviewer<input type="checkbox"/> Organisation User<input checked="" type="checkbox"/> SIRO 
Name: (forename Surname)	<input type="text"/>	
Password: (case sensitive)	<input type="password"/>	
Confirm Password:	<input type="password"/>	
Email:	<input type="text"/>	
Telephone:	<input type="text"/>	
Email User Account Details:	Use General User Template <input type="text"/>	

Rules for entering passwords are as follows:

- Must be at least 6 characters long.
- Must contain both numeric and alphabetic characters.
- Should not contain dates.
- Should not contain the organisation name.
- Must not be the same as the Organisation Code or your User ID
- Must not contain 2 consecutive identical characters. For example, the password LOOK78B4 would be invalid as it contains the same character "O" side by side, or consecutively.
- Must not be a password previously used within the last year.

Page Processing Time: 0.03 seconds
Page Render Time: 0.16 seconds

Once the role is added and the SIRO is logged in a new option of Cyber Security will be displayed on the left-hand menu and the survey can be launched from there.

You are here: Cyber Security

Cyber Security Preparedness

[Log Out](#)

- Home
- News
- CyberSecurity**
- Change Requests
- Reports
- Resources
- Admin
- Publications
- Help

Facing the Cyber Security Challenge

Over the years we have asked you how you meet the security challenge measured through the IG toolkit and when applying for N3 connections. The core principles such as secure remote working, information assets register and governance for information lead by the SIRO are increasingly important, now more than ever.

Every day around the world, thousands of IT systems are compromised. Some are attacked purely for the *kudos* of doing so, others for political motives, but the most commonly to steal money or sensitive information.

Traditionally, for the NHS and Local Government organisation, IT infrastructure has primarily resided on private networks and the organisation has had access to information on National Systems or from other organisations sat on the same private network (such as N3 & PSN).

The move to enable greater access to patients and service users (such as patient portals), married to the cost effectiveness of cloud / software as a service, has meant more external facing or hosted systems. Where we may have thought we would not be affected by cyber activity due to being internal facing, this may no longer be the case.

Now is a good time to think about our approach to protecting our information assets in light of the cyber challenge that faces us all and review the controls *in situ*.

Controls can come in many forms ranging from contractual assurance from your provider, technical penetration testing / application vulnerability and system level security policies.

The threats and controls are not new and build on the good work already undertaken; however the likelihood of cyber related incidents has increased. Your information governance toolkit assessment provides a framework for capturing and managing your response. The link to the factors and guidance material are shown beneath the launch survey link.

The survey is a mixture of multiple choice responses and free text fields for some responses.

The survey is designed to help us and you to gauge your organisation's cyber preparedness. The results of this survey will be used to identify where improvements in guidance, tools and services can be made to assist organisations across Health and Social when tackling the Cyber Security Challenge.

[Launch The Survey](#)

It is envisaged that input from other staff members will be required to assist the SIRO to complete the survey, so there is a facility to save any progress made. When complete, the survey should be published. Once published, the results are available to the HSCIC and the SIRO can view their completed responses.