Incident Response Guide Introduction

Scottish Business
Resilience Centre

Incident Response Guide Introduction

Developing an incident response plan is a critical step towards preparing a robust and effective incident management and technical response capability. Good incident management will help reduce the financial and operational impact on your business.

Information for planning and responding to a cyber incident can be found at

https://www.cyberscotland.com/incident-response/

Use these supporting documents to help you plan your response to a cyber incident.

Prepare Your Business Checklist:

Use this checklist to help prepare for, respond and recover from cyber incidents.

Emergency Contact List Template:

Use this document to capture business emergency contact details. Include staff names and contact details, emergency contacts, customers and supplier details. Make a digital copy of the document available in a place you can access it easily. Print a hard copy of the document and keep it in a safe place.

Clarktech.

Incident Response Communications:

Core questions you need to address when planning and dealing with a crisis.

CMS law·tax·future

Legal Implications of a Cyber Incident:

Awareness of the key commercial and legal implications of a cyber incident is crucial to responding appropriately to any incident and mitigating the risks arising from it. In this document you will find points to consider, to help ensure the decisions you take during and in the aftermath of a cyber incident enable you to navigate out of choppy waters with minimal damage.

Additional advice to improve your cyber resilience
https://www.cyberscotland.com/advice-and-guidance/

Get a list of actions to improve your security using the Cyber Aware Action Plan

Take steps to increase your protection using the NCSC's Small Business Guide:

- [ ] Backing up your data
- [ ] Protecting your organisation from malware
- [ ] Keeping your smartphones (and tablets) safe
- [ ] Using passwords to protect your data
- [ ] Avoiding phishing attacks
- [ ] NCSC's Response and Recovery Guide

Consider Cyber Essentials certification to improve your organisations resilience.

- [ ] The Cyber Essentials Readiness Tool helps you move towards meeting Cyber Essentials requirements. The tool includes questions related to the main Cyber Essentials criteria and provides advice to prepare for certification.

Follow data protection guidance

- [ ] Information Commissioner's Office – find out about your obligations and how to comply, including protecting personal information and provided access to official information.

Be aware of current cyber security threats and techniques

- [ ] Sign up to Cyber Information Sharing Partnership (CISP)
- [ ] Register to receive information about threats on your network with the National Cyber Security Centre Early Warning Service
- [ ] Keep up to date on NCSC news
- [ ] Sign up to the CyberScotland newsletter

Scottish Business Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

01786 447 441
enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland