# CYBER INCIDENTS RESPONSE PLAN

Dalmuir Park Housing Association

Your Future Our Future

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

# Contents

## 1.0 CYBER INICIDENT RESPONSE PLAN (CIRP)

A Cyber Incident Response Plan (CIRP) ensures an effective response and prompt recovery in the event security controls do not prevent an incident occurring.

Cyber security are measures used to protect the confidentiality, integrity and availability of systems and information. A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, which have a significant probability of compromising business operations.

As adversaries become more adept, the likelihood and severity of cyber-attacks is also increasing due to the interconnectivity and availability of information technology platforms, devices and systems exposed to the internet.

## 2.0 CIRP OBJECTIVES

- To provide guidance on the steps required to respond to cyber incidents.
- To outline the roles, responsibilities, accountabilities, and authorities of personnel and teams required to manage responses to cyber incidents.
- To outline legal and regulatory compliance requirements for cyber incidents.
- To outline internal and external communication processes when responding to cyber incidents.
- To provide guidance on post incident activities to support continuous improvement.

## 3.0 STANDARDS AND FRAMEWORKS

The relevant standards and frameworks used to inform the CIRP include:

- International standards and frameworks:
    - NIST Computer Security Incident Handling Guide
    - International Standard ISO/IEC27035-1
    - International Standard ISO/IEC 27035-2
    - International Standard ISO/IEC 27035-3

- Organisational Guidance:
    - The National Cyber security Centre
    - Information Commissioner's Office
    - CyberScotland
    - Scottish Government (Cyber Resilience)

## 4.0 INCIDENT RESPONSE PROCESS

## 5.0 REPORTING CYBER INCIDENTS

All incidents must be reported to the first point of contact and if unavailable the second point of contact and so on:

| Name | Contact Details | Areas of Responsibility |
|---|---|---|
| CEO | 07908012871(W) | Overall responsibility |
| Finance and Corporate Services Manager | 07960481624 (W) | Finance and Corporate Services & responsible for the overall responsibility in the absence of CEO. |
| Customer Service Manager | 07903315410(W) | Customer Services |
| Care Service Manager | 07930401531(W) | Care Services and DOSCG |

- Although The Leadership Team have overall responsibility for their area, tasks will be delegated to various staff team.

| EXTERNAL CONTACTS | | |
|---|---|---|
| **Role** | **Responsibility** | **Contact** |
| Managed IT service provider/ IT provision | Finance Services Officer | Microtech 01563 530480 Support Manager (Kenny Spelman) for major issues to Direct Level (Paul Mathewson) |
| Insurance providers | Finance and Corporate Services Manager/Senior Finance Services Officer | Howden Insurance Brokers Stacy Barrett 0141 354 2899 |
| Website providers | Corporate Services Team | Microtech 01563 530480 |
| Regulators | CEO/Leadership Team | Scottish Housing Regulator<br>OSIC<br>Care Inspectorate |
| ICO | CEO/Leadership Team/DPO/Corporate Services Officer | Tel: 0303 123 1113 |
| Cyber and Fraud Centre Scotland | CEO/Finance and Corporate Services Manager | Incident Response Helpline 0800 1670 623 |

## 6.0 Severity Matrix

The Leadership Team and Microtech can use the below table to classify the severity of the cyber incidence. The severity should imply the speed and importance of your response.

| Severity | Examples |
|---|---|
| **Critical** | • Over 80% of staff (or several critical staff/teams) unable to work<br>• Critical systems offline with no known resolution<br>• High risk to / definite breach of sensitive client or personal data<br>• Financial impact in excess of £1million<br>• Severe reputational damage - likely to impact business long term |
| **High** | • 50% of staff unable to work<br>• Risk of breach of personal or sensitive data<br>• Noncritical systems affected, or critical systems affected with known (quick) resolution<br>• Financial impact between £250k to £1million<br>• Potential serious reputational damage |
| **Medium** | • 20% of staff unable to work<br>• Possible breach of small amounts of non-sensitive data<br>• Low risk to reputation<br>• Small number of non-critical systems affected with known resolutions<br>• Financial Impact between £50k to £250k |
| **Low** | • Minimal, if any, impact<br>• Financial impact less than £50k |

[Financial loss figures have been taken from DPHAs Strategic Risk Register - Risk Appetite & Risk Tolerance Scoring Matrix]

## 7.0 COMMUNICATING CYBER INCIDENTS

| No | Action | Who |
|---|---|---|
| 1 | • Assess if Insurance Broker needs to be advised. | CEO, Leadership Team, Senior Finance Services Officer |
| 2 | • Contact agencies as necessary:<br>- Police Scotland<br>- Scottish Housing Regulator (notifiable event).<br>- Information Commissioners' Office (Data Breach)<br>• Managers will contact their staff to advise them about the situation and what employee expectations.<br>• Assess whether Board of Management requires it to be advised.<br>• Assess if contact with the media is required.<br>• Assess if customers need to be advised and the website and social media sites are updated.<br>• Assess if contractors need to advise. | CEO, Leadership Team |
| 3 | • Internal Communication to include:<br>- A brief summary of the incident and business impact.<br>- Actions currently being undertaken to resolve the incident.<br>- Actions staff can take to assist.<br>- Business continuity options for staff who are affected by the incident.<br>- Messaging for customers / contactors<br>- Key points of contact for enquiries<br>- Expected timeframes for further updates. | CEO, Leadership Team |
| 4 | • External Communication to include:<br>- System/services affected.<br>- Steps being taken to resolve the incident.<br>- Who your organisation is working with to support incident remediation.<br>- Options for stakeholders affected by the incident (customers)<br>- Key points of contact for enquiries | CEO, Leadership Team |

| | | |
|---|---|---|
| | - Expected timeframes for further updates.<br>- Liaise with Insurance Company, IT Consultant, DPO for next steps ensuring best practice is followed and best outcome for the Association is had.<br>- Insurance brokers have confirmed that DPHA complies with the noted controls and processes underwritten in the Cybersafe Insurance document | |

## 8.0 COMMON THREATS

| Type | Description |
|---|---|
| **External/ Removable Media** | An attack executed from removable media or a peripheral device (e.g., malicious code spreading onto a system from an infected USB flash drive). |
| **Attrition** | An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS attack intended to impair or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords). |
| **Web** | An attack executed from a website or web-based application (e.g., a cross- site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware). |
| **Email** | An attack executed via an email message or attachment (e.g., exploit code disguised as an attached document or a link to a malicious website in the body of an email). |
| **Supply Interdiction** | An antagonistic attack on hardware or software assets utilising physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer. |
| **Impersonation** | An attack involving replacement of something benign with something malicious (e.g., spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation). |
| **Improper usage** | Any incident resulting from violation of an organisation's acceptable usage policies by an authorised user, excluding the above categories (e.g., a user installs file sharing software, leading to the loss of sensitive data). |
| **Loss or Theft of Equipment** | The loss or theft of a computing device or media used by an organisation (e.g., a laptop, smartphone or authentication token). |
| **Unauthorised Access** | Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account. |

## 9.0 COMMON CYBER INCIDENTS AND RESPONSE ACTIONS

The following is a list of common cyber incident types and corresponding initial response actions.

### Definition of Ransomware:

Ransomware is a form of malicious software (malware) that enables cyber criminals to remotely lock down or encrypt the files on your device. Criminals use ransomware to extort money from you (a ransom) and will claim to restore access to your files or device once you have paid. Ransomware can be delivered in various ways; for example, via attachments in authentic looking emails purporting to be from genuine companies.

**Detection & Identification**

- Identify symptoms of a ransomware infection (e.g., locked files, ransom note pop-up, system slowdown).
- Isolate the affected system immediately by disconnecting it from the network to prevent further spread.
- Do not restart or power off the system until memory forensics (if applicable) can be performed.

**Response:**

**Containment & Mitigation**

- Notify the IT security team / incident response team immediately.
- Document everything – time of discovery, affected systems, error messages, ransom notes.
- Secure backup copies – ensure backups are disconnected/offline and verified to be clean.
- Preserve evidence – retain logs, email headers, ransom note, encrypted files for forensic analysis.

**Eradication & Recovery**

- Run full anti-malware tools to scan the environment (but only after isolation).
- Rebuild infected machines from clean images – do not trust “decrypted” systems.
- Restore files from a verified clean backup if available.
- Patch and update operating systems, applications, and antivirus signatures.

**Communication & Notification**

- Do not engage with the attacker unless instructed by law enforcement.
- Report to authorities:

  Action Fraud (UK): https://www.actionfraud.police.uk

  NCSC (if serious national impact): https://report.ncsc.gov.uk
- Notify the ICO within 72 hours if personal data is involved (GDPR requirement).

**Post-Incident Activities**

- Conduct a root cause analysis and determine how the infection occurred.
- Update policies and user awareness training.
- Review firewall rules, email filtering, remote desktop configurations, and disable unnecessary services

## Definition of Malware

Malware (malicious software) is any software intentionally designed to cause damage, steal data, disrupt services, or gain unauthorised access to systems. This includes:

- Viruses – attach themselves to files or programs and spread when those files are opened.
- Trojans – appear to be legitimate software but carry malicious payloads.
- Worms – self-replicating and spread through networks without user action.
- Spyware, adware, keyloggers, and rootkits may also fall under malware categories.

**Common Signs of a Malware-Infected Device**
(These are good and should be retained, but refined for clarity)

- Unusual system slowness or freezing
- Automatic restarts or shutdowns
- Unexpected program or app behaviour
- Pop-up windows or fake alerts from unknown programs
- Strange emails or messages sent from your account
- Phone calls or emails claiming to be from “Microsoft” or “your ISP” demanding access or payment
-

**Detection and Initial Response**

- Do not interact with suspicious pop-ups or links.
- Isolate the device from the network immediately (turn off Wi-Fi, unplug Ethernet, disable Bluetooth).
- Do not power off the device unless advised by IT (to preserve volatile evidence).
- Notify your internal IT/security contact or service desk immediately.
- Do not attempt to remove malware yourself unless authorised and trained.

**Containment**

- Quarantine the device – either physically isolate it or use endpoint protection tools.
- Log the incident: date/time detected, symptoms, any suspicious files or emails.
- If you received a fake support call, hang up and do not provide payment or allow access.
    - If payment was made, contact your bank or card provider immediately.
    - Report the scam to Action Fraud and/or Police Scotland.

**Eradication**

- If authorised by IT/security:
    - Run a full anti-virus/anti-malware scan.
    - Delete or quarantine infected files as instructed.
    - Apply security patches and updates to OS and software.
- If scans do not resolve the issue:
    - Rebuild from a clean image or backup (factory reset only if no better alternative and device is not enterprise-managed).

**Recovery**

- Reconnect the system to the network only after clearance from IT/security.
- Monitor the system for abnormal activity.
- Reset relevant passwords (especially if credential theft is suspected).
- Restore data from verified backups (if applicable).

**Reporting & Follow-up**

- Report internally via your organisation's incident response process.
- If personal data is involved, Data Protection Officer (DPO) must assess and potentially report to the ICO within 72 hours (GDPR requirement).
- Log all actions taken for audit, legal, and insurance purposes.
- Conduct a post-incident review to assess:
    - Entry vector
    - Prevention gaps
    - User training needs

## Definition of DOS/DDOS

A **Denial of Service (DoS)** attack is an attempt to make a system, service, or network resource unavailable by overwhelming it with traffic or requests. A **Distributed Denial of Service (DDoS)** attack amplifies this impact by using multiple compromised devices or systems (a botnet) to generate the traffic, often making the attack harder to block or trace. The goal is typically to disrupt operations, damage reputation, or distract from other attacks.

**Response:**

**Indicators of a DoS or DDoS Attack**

- Websites, VPNs, or cloud services suddenly become unreachable or extremely slow.
- Internet bandwidth appears saturated with no legitimate activity.
- Unusual traffic spikes from a single IP address range or many sources globally.
- Multiple systems reporting lost internet or service connections at once.

**DoS/DDoS Response Procedure/ Detection and Initial Assessment**

- Confirm the nature of the disruption:
    - Is it a connectivity issue, hardware failure, or attack?
    - Check firewall/router logs for unusual incoming traffic patterns.
    - Use external monitoring services (where available) to verify website or service reachability from outside.

**Immediate Containment**

- Switch to backup internet line (e.g., FTC 80/20 on DrayTek Router) via predefined failover config.
    - Ensure this change is tested regularly and documented.
- Divert voice services to backup SIP trunk.
- Activate 4G hubs or mobile broadband as emergency internet for critical services (e.g., email, remote access).
- Isolate non-essential systems from consuming available bandwidth.
- Engage the ISP's abuse/security department to:
    - Identify the attack type (volumetric, protocol-based, application-layer).
    - Apply network-level blocking or blackholing.
    - Assist with traffic rerouting or scrubbing.

**Escalation and Communication**

- Notify:
    - Internal IT/security leads
    - Your ISP (e.g., Virgin Media) for upstream mitigation
    - Managed Security Provider, if applicable

- If attack is sustained or high impact:
    - Notify **NCSC** via https://report.ncsc.gov.uk
    - Log incident for **Action Fraud** if suspected to be part of wider criminal activity.

**Recovery and Service Restoration**

- Monitor when attack subsides or is mitigated.
- Gradually reconnect primary infrastructure in stages (main switch, fibre broadband).
- Test availability of:
    - Voice services
    - Internal systems
    - External-facing websites and cloud services
- Perform log reviews to understand timeframes and sources.

**Post-Incident Review & Resilience**

- Assess:
    - What systems/services were impacted?
    - Did failover work effectively?
    - Were customers or third parties affected?
- Improve:
    - ISP DDoS mitigation contract or SLAs
    - Rate-limiting and geo-blocking on firewalls
    - Load balancing, content delivery networks (CDNs), and cloud-based DDoS protection (e.g., Cloudflare, Azure DDoS Protection)
- Include DDoS response in your business continuity testing.

**DOS/Cyber Attack on Internet Service Provider (Virgin Media)**

## Definition of Phishing

**Phishing** is a type of social engineering attack in which an attacker sends fraudulent messages (typically via email or SMS) designed to trick users into revealing sensitive information (e.g., passwords, financial data) or to click links/download attachments that install malware or create a backdoor for remote access.

Phishing may take several forms:

- Spear phishing: targeted at specific individuals or roles
- Whaling: aimed at senior executives
- Clone phishing: mimicking legitimate communications
- Vishing: voice-based phishing (e.g., phone calls)

**Common Indicators of Phishing Emails**

- Urgent tone (“your account will be closed”)
- Unexpected attachments or links
- Sender email domain mismatch or misspellings
- Request for personal, financial, or login information
- Promises of money, refunds, or prize winnings
- Slightly altered but familiar display names

**Response:**

**Phishing Response Procedure**

**Detection & Initial User Action**

- Do not click on any links or download attachments.
- Do not reply to the message or forward it to others.
- Report the email immediately using your organisation's reporting process (e.g., "Report Phishing" button or dedicated email).
- If already clicked or credentials were entered, report this explicitly.

**Internal Containment & Notification**

- IT/Security team should:
    - Isolate the affected user account and device (network disconnection if suspicious behaviour is observed).
    - Reset affected credentials immediately.
    - Notify all staff of the phishing attempt, including:
        - Screenshots or redacted examples
        - Key signs to look out for
    - Reinforce that external emails are marked (confirm with IT/MSP this feature is live and working).

**Technical Controls**

- Request your IT provider (e.g., Microtech or internal team) to:
    - Block the sender's email domain or IP at the email gateway or spam filter.
    - Add any malicious links or attachments to blocklists.
    - Check logs for other users who received or clicked the email.

**Investigation & GDPR Compliance**

- Determine:
    - Whether the phishing attempt was successful (e.g., credential compromise, malware installed).
    - If any unauthorised access occurred using stolen credentials.
    - If personal or sensitive data has been exposed.

- If a **data breach** has occurred:
    - Follow the UK GDPR breach response protocol.
    - Report to the ICO within 72 hours if required.
    - Notify affected individuals where appropriate.

**Device & Malware Checks**

If malware is suspected (e.g., file download occurred):

- Disconnect the device from the network.
- Run a full antivirus/malware scan.
- Do not factory reset unless advised and no recovery is possible.
- If infection persists:
    - Rebuild from a clean image.
    - Seek support from IT/Security or your MSP (e.g., Microtech).

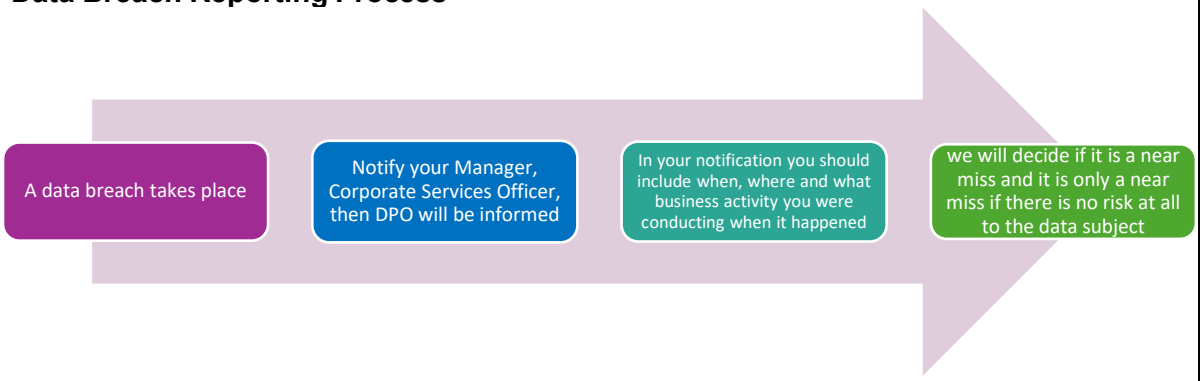
**Awareness & Preventative Action**

- Include **phishing awareness training** in all staff GDPR & security training sessions.
- Regularly simulate phishing tests to assess awareness.
- Update Acceptable Use and Incident Response policies based on lessons learned.

**Data Breach**

A data breach occurs when sensitive or personal information is accessed, disclosed or exposed to unauthorised people. This may be by accident, or the result of a security breach. For example, when an email with personal information is sent to the wrong person, or a computer system is hacked and personal information is stolen.

**Data Breach Reporting Process**




**Response:**

1. Corporate services officer (CSO) to discuss with Data Protection Officer (DPO)
2. They recommend/decide external parties to notify
   - Insurance company (SFSO or CSO) – cyber only
   - Data subjects affected (tenants or staff) (Housing Officer or CSO) - any high-risk breach
   - ICO ( DPO reports) – High risk only (within 72 hours) ICO **helpline on 0303 123 1113**
   - NCSC and or Police (CSO/DPO) - cyber or fraud only
3. If Cyber Event stand up emergency incident group ( CSO, SFSO, IT provider, DPO, Insurance assessors)
4. Update the Breach Register including any “near misses” and note any remedial action taken.
5. Take remedial actions to recover situation
   - If possible, recover data, do so immediately.
   - Any stolen laptop or iPads and mobiles, remotely wipe using Intune.
   - If required manage affected staff members passwords.
   - Consider additional technical security measures , such as access controls, penetration testing, firewall security, email checking software and password refresh policy
   - Staff awareness and training
   - One to one review with person who caused breach
   - Review of processes to improve data loss prevention

| **Unauthorised access** |
| --- |
| **Response:**<br>1. Reporting Cyber Incidents – see section 6.0.<br>2. Keep the system running in the state it was when the compromise was detected.<br>3. Notify users of the computer, if any, of a temporary service interruption.<br>4. It is important that NO further commands or actions be taken on the related Information System. Doing so may destroy relevant forensic data and impede ISO investigations.<br><br>**DO NOT:**<br>- Scan the system with antivirus software.<br>- Attempt to clean off any malicious software.<br>- Attempt to clear the mail system.<br>- Attempt to retract an email message that contained confidential data<br>- Run a backup. |

## 10.0 DPHA SECURITY & DISASTER SUMMARY

**Annual Cyber-Security Testing –** Microtech carry out an annual Network Penetration test.

**Anti-Virus and Security Update Management -** AV and Security solutions are in place and are managed and updated by Microtech.

**Windows Updates / Patch Management Firewall -** patching and software updates are in place and are managed by Microtech for Computers and Network devices

**Additional PC & Mobile Device Security File / Server Backup -** Server backups are in place and are monitored and managed by Microtech

**Office 365 back up -** Microtech manage and monitor Office 365 backups included Email, SharePoint, Teams and OneDrive.

**Email SPAM Filter -** in place.

**Annual Disaster Recovery Testing Backup –** in place.

**Disaster Recovery Premises & Hardware -** Agreement in place that in DR scenario users can work from home or alternative locations. Already up and running and Microtech would assist if there were any issues.

**Broadband & Telephony Infrastructure -** The solutions have resilience and backup connections.

**Multi-Factor Authentication -** in place across all systems where available.

**Office Wi-fi – guest password/staff password -** two networks exist with separation to ensure guest and work do not use same networks.

**Lessons learned –** In the event of a cyber incident, a staff session will be held within one month to discuss the incident, share lessons learned and identify any necessary training. This would be facilitated by an expert in the relevant field.