Cyber-continuity and Incident
RESPONSE PLAN TOOLKIT

Macbeth

Table of Contents

Introduction

While the vast majority of organisations have implemented a business continuity plan (BCP) into their framework, many don't possess a management plan specific to cyber-risks, also known as a cyber-continuity and incident response plan. Between the abundance of high-profile data breaches that have occurred in the past couple years, such as Facebook, British Airways or TalkTalk, and strict data protection requirements by the UK General Data Protection Regulation (GDPR), failing to account for cyber-exposures in your organisation's BCP is a risk you simply cannot afford to take.

When a data breach or other cyber-event occurs, the damages can be significant, often resulting in legal actions, fines and serious financial losses. What's more, cyber-exposures impact businesses of all kinds, regardless of their size, area of focus, or status as a private or public entity.

Even the most secure organisations are at risk of a data breach. Indeed, recent data from the Department for Digital, Culture, Media & Sport found that 39 per cent of UK businesses and 30 per cent of charities suffered a data breach in the past year. And that's just what we know about. It can often take days or even months for a company to notice its data has been compromised. And, when it comes to containing the damage caused by a data breach, having a response plan in place is crucial.

While cyber-security programmes help secure an organisation's digital assets, cyber-continuity and incident response plans provide comprehensive, proactive guidance for organisations to prevent cyber-threats, as well as reactive steps for companies to follow when a cyber-event occurs. Utilising a continuity and response plan allows organisations to ensure business success throughout any cyber-scenario, notify impacted customers and partners quickly and efficiently, and limit financial and reputational damages.

Timely responses to breaches are increasingly important when you consider that, according to a recent report sponsored by IBM Security, organisations that contain a breach in less than 30 days save an average of £1.4 million. Indeed, every second counts—recent research from the Ponemon Institute revealed that nearly 5 million data records are lost or stolen every day, totalling 58 records each second. And considering the cost of the average data record is over £100, wasted time can quite literally become wasted money during a breach.

In addition, the Ponemon Institute's research found that implementing proper business continuity management practices can reduce the average cost of a data breach by nearly £500,000. Essentially, failing to have a clear plan in place that ensures immediate action in the face of a breach could cost an organisation millions of pounds and shatter its reputation.

This toolkit provides organisations with a general overview of cyber-continuity and incident response plans—what they are, their benefits, how to implement them, how they can help organisations meet the increasing demands of data protection laws, such as the GDPR, and how they can ensure overall business continuity. While organisations may approach cyber-security differently depending on their unique exposures and the kind of data they store, this resource provides a number of best practices to keep in mind.

Why Cyber-continuity and Incident Response Plans Matter

Simply put, every organisation that stores or handles data is at risk of a cyber-attack. As technology advances, companies are collecting, storing and transferring more personal information about their customers and employees than ever before. This not only puts a target on an organisation's back, but it also means that just one breach can affect thousands or even millions of individuals. And, unfortunately for businesses, cyber-incidents cost more than just data:

- Data breaches are becoming increasingly expensive. While cyber-liability insurance can help offset the costs of a data breach and any subsequent litigation, just one breach can be financially devastating. According to a survey conducted by the Ponemon Institute, the average cost of a data breach was £4.5 million, or £200 per lost or stolen record.
- Non-compliance fines can be significant. Under the GDPR, organisations that fail to comply with the law have the potential to suffer hefty fines from the Information Commissioner's Office (ICO). Serious violations can result in fines of up to £17.5 million, or 4 per cent of turnover (whichever sum is greater).
- Cyber-incidents can lead to serious reputational damage, significantly impacting directors and officers. Reputational damages can easily reach six figures. According to Kaspersky Lab, a global cyber-security company, a single cyber-incident caused brand damage of £6,300 for small and medium-sized businesses and £156,500 for larger organisations. When wide-scale breaches occur, a company's reputation can be tarnished, sometimes permanently. In addition, the public holds organisations accountable for major losses of personal data, and directors and officers are often the ones who take the blame.

The Benefits of a Cyber-continuity and Incident Response Plan

Most organisations have some form of data protection in place. While these protections are critical for minimising the damages caused by a breach, they don't provide clear action steps following an attack. That's where cyber-continuity and incident response plans can help.

Cyber-continuity and incident response plans are written guides comprised of instructions, procedures and protocols that enable an organisation to respond to and recover from various kinds of data security incidents. Cyber-attacks are no longer a matter of if, but when, and reacting to an inevitable breach takes more than just threat neutralisation.

Companies must have the ability to respond to and defend against evolving threats. Cyber-continuity and incident response plans give organisations the tools they need to further enhance their data protection practices as well as help them:

1. Anticipate cyber-security incidents before they occur.
2. Minimise the impact of cyber-security incidents.
3. Mitigate threats and vulnerabilities while a cyber-attack occurs.
4. Improve cyber-security response overall, encouraging buy-in at a management level.
5. Reduce the direct and indirect costs caused by cyber-security incidents.
6. Maintain business continuity in the face of major threats.
7. Prevent the loss of data critical to their business.
8. Improve the overall security of their organisation.
9. Strengthen their reputation as a secure business, increasing customer confidence.
10. Devote more time and resources to business improvements, innovation and growth.

Above all, cyber-continuity and incident response plans can help organisations better understand the nature of an attack, which, in turn, promotes a fast and thorough response to threats. However, cyber-continuity and incident response plans are typically created and implemented as part of larger cyber-security programmes. As such, it's important for businesses to have a basic understanding of what goes into creating an effective cyber-security programme.

Cyber-continuity and Incident Response Plans: Part of Larger Cyber-security Programmes

In a general sense, a cyber-security programme establishes a framework that allows businesses of all sizes to be proactive when it comes to cyber-threats and attacks.

Cyber-continuity and incident response plans, however, are just one component of cyber-security programmes. While companies can have a cyber-continuity and incident response plan without implementing an overall cyber-security programme, it's not advised. This is because cyber-security programmes are one of the best weapons companies have to focus on cyber-security initiatives and limit the impact of data breaches.

Cyber-security programmes may vary from business to business, but they generally include the following:

1) Top-down Involvement

Many wrongly assume that IT departments are solely responsible for managing data risks and ensuring cyber-security across an organisation. In order for businesses to protect themselves, management must also play an active role. Not only does involvement from leadership improve cyber-security, it can also reduce liability for directors and officers. Asking thoughtful questions can help management better understand the strategies IT uses to prevent, detect and respond to data breaches. When it comes to cyber-threats, organisations need to be diligent and thorough in their risk prevention tactics, and management can help move the cyber-conversation in the right direction. To help oversee their organisation's cyber-risk management tactics, management should ask:

1. Does the organisation utilise technology to prevent data breaches? Every company must have robust cyber-security tools and antivirus systems in place. These systems act as a first line of defence for detecting and preventing potentially debilitating breaches. While it may sound obvious, many organisations fail to take cyber-threats seriously and implement even the simplest protections. Boards can help highlight the importance of cyber-security, ensuring that basic, preventive measures are in place.
2. Has the company's management team identified a senior member to be responsible for organisational cyber-security preparedness? Organisations that fail to create cyber-specific leadership roles could end up paying more for a data breach than organisations that do. This is because, in the event of a cyber-incident, fast response and clear guidance is needed to contain a breach and limit any damages. In addition, the GDPR requires organisations to appoint a Data Protection Officer (DPO) if the organisation is a public authority, if their core activities consist of data processing or if their core activities consist of large-scale processing of special categories of data or personal data relating to criminal offences. A DPO reports to the highest management level and has a responsibility to advise the organisation of their data protection obligations, monitor the organisation's compliance with the GDPR, advise on whether a data protection assessment is needed, serve as a contact point on all data protection issues (including data breach reporting) and act as data subjects on privacy matters (such as for subject access requests).When establishing a DPO or similar cyber-leadership role, management needs to be involved in the process. Cyber-leaders should have a good mix of technical and business experience. This individual should also be able to explain cyber-risks and mitigation tactics at a

high level so they are easy to understand for those who are not well-versed in technical terminology. It should be noted that smaller organisations may not have an in-house cyber-specialist. In these instances, organisations must still identify a qualified team member to help co-ordinate cyber-initiatives and breach response practices.

3. **Has the organisation discussed and formalised a cyber-risk budget? How engaged is management in terms of providing guidance related to cyber-exposures?** Both overpaying and underpaying for cyber-security services can negatively affect an organisation. Creating a budget based on informed decisions and research helps companies invest in the right tools. Management can help oversee investments and ensure that they are directed towards baseline security controls that address common threats. Management, with guidance from the DPO or a similar cyber-leader, should also prioritise funding. That way, an organisation's most important assets are protected.
4. **Does the organisation have a system in place for staying current on cyber-trends, news and data security regulations?** Cyber-related legislation can change with little warning, often having a sprawling impact on the way organisations do business. If organisations do not keep up with data security regulations, they could face serious fines or other penalties.
5. **Has the organisation conducted a thorough risk assessment? Has the organisation purchased or considered purchasing cyber-liability insurance?** Cyber-liability insurance is specifically designed to address the risks that come with using modern technology—risks that other types of business liability cover simply won't cover. The level of cover your business needs is based on your individual operations and can vary depending on your range of exposure. As such, businesses need to conduct a cyber-risk assessment and identify potential gaps. From there, organisations can work with their broker to customise a policy that meets their needs.

While it's important for management to provide adequate oversight, carrying out cyber-security initiatives is ultimately up to a company's appointed leadership. Above all, management must make sure that directors and officers clearly understand their roles and responsibilities:

GENERAL RESPONSIBILITIES OF DIRECTORS AND OFFICERS	
Policies	• Adopt written cyber-security policies, procedures and internal controls. • Implement tools that detect cyber-security events.
Appointments	• Discuss (at the management and board level) the hiring of a DPO or similar role. Hiring a DPO or creating a new cyber-leadership role is not practical for every business. In these instances, organisations should identify a qualified, in-house team member and roll cyber-security responsibilities into their current job requirements.
Reviews and Reports	• Review budgets and IT security programmes annually. • Receive and review reports on any data incidents. • Remain well-informed on cyber-security trends that could impact the business. • Create and oversee a team of individuals who are responsible for cyber-security oversight.
Direction	• Assess cyber-security risks, determining which risks can be mitigated directly and which may be transferred using cyber-liability insurance or other cover.

2) Training and Policies

Every cyber-security programme must address employee training and create cyber-security policies. The content of these policies will differ depending on the size and type of the organisation, but typically include similar elements. The checklists below identify questions organisations should ask in order to establish or adjust companywide policies regarding cyber-security:

POLICIES	YES	NO	N/A
Does your organisation have a cyber-security policy in place?	☐	☐	☐
Is your organisation's cyber-security policy enforced?	☐	☐	☐
Does your organisation's cyber-security policy include an internet access policy?	☐	☐	☐
Does your organisation's cyber-security policy include an email and communications policy?	☐	☐	☐
Does your organisation's cyber-security policy include a remote access policy?	☐	☐	☐
Does your organisation's cyber-security policy include a "bring your own device" (BYOD) policy?	☐	☐	☐
Does your organisation's cyber-security policy include an encryption policy?	☐	☐	☐
Does your organisation's cyber-security policy include a data breach response policy?	☐	☐	☐

PERSONNEL SECURITY	YES	NO	N/A
Does your organisation have a system in place for checking the background of employees and contractors that have access to computer systems and sensitive data?	☐	☐	☐
Are employees and contractors required to wear ID badges?	☐	☐	☐
After an employee or contractor is no longer authorised to conduct work on your organisation's behalf, do you revoke access to your computer systems?	☐	☐	☐

PHYSICAL SECURITY	YES	NO	N/A
Does your organisation ensure the physical security of its computer systems?	☐	☐	☐
Are personal computers inaccessible to unauthorised users?	☐	☐	☐
Are there procedures in place to keep computers from remaining logged in for prolonged periods of time?	☐	☐	☐
Does your organisation have a process for notifying IT personnel if a device is misplaced or stolen?	☐	☐	☐

SECURITY AWARENESS AND EDUCATION	YES	NO	N/A
Is your staff informed regarding the importance of computer security?	☐	☐	☐
Does your organisation provide employees with cyber-security training on a regular basis?	☐	☐	☐
Are your staff members familiar with techniques they can use to prevent a security breach?	☐	☐	☐
In the event of a data breach, does your staff know how to respond? (This includes notifying the ICO within 72 hours of the data breach occurrence.)	☐	☐	☐
Do your staff members know how to keep their passwords and hardware secure?	☐	☐	☐

3) IT Security

One of the most important aspects of a cyber-security programme are IT defences themselves. Above all, organisations want to invest in the right solutions—solutions that are adequate and up to date. Organisations should install industry-standard antivirus and malware protections, documenting any and all updates. It's also important that your network is protected against internal and external attacks as much as possible. You should secure wireless networks using firewalls, malware detection and similar protections. Conduct penetration testing regularly and make sure that technical solutions are in place to detect and block suspicious activities or access. The checklist below outlines some general questions organisations should ask to promote thorough and comprehensive IT security:

IT PROCEDURES	YES	NO	N/A
Does your organisation keep operating systems and antivirus software up to date?	☐	☐	☐
Does your organisation periodically perform vulnerability scans on servers and all the computers used in your organisation?	☐	☐	☐
Does your organisation patch the software on all systems by following a regular schedule?	☐	☐	☐
Are employees required to create strong passwords?	☐	☐	☐
Does your organisation encrypt sensitive data?	☐	☐	☐
Does your organisation have a process for retrieving backup and archival copies of critical data?	☐	☐	☐
Does your organisation have policies and procedures in place for handling credit card and other personal private information?	☐	☐	☐
Does your organisation have "secure send" procedures in place so it can receive and distribute client information safely?	☐	☐	☐

Cyber-security Programmes: A Continual Process

Creating a cyber-security programme is an involved process, and there is no one-size-fits-all solution. In fact, certain organisations may have more detailed programmes depending on the scope of their IT infrastructure and the type of data they handle for customers, partners and employees.

While basic considerations are outlined above, organisations will want to perform regular risk assessments to help them determine what specific steps to take when crafting a cyber-security programme.

Qualified insurance brokers can help you understand your cyber-risks and provide you with a list of key business areas to examine. Cyber-security programmes should evolve alongside the threat landscape, and you will need to update policies, IT protections and training information as needed.

The 5 Phases of Cyber-continuity and Incident Response Plans

While cyber-continuity and incident response plans will differ based on a company's size, assets and industry, they contain similar elements. All plans should be:

1. Prepared in advance, with continuity in mind
2. Detailed
3. Tested
4. Understood by those within the organisation
5. Drafted with industry best practices in mind

Continuity and response plans help focus the efforts of many individuals before, during and following a cyber-incident and should be the result of input from stakeholders across the company. When establishing a cyber-continuity and incident response plan, it's best to think in phases.

Phase 1: Plan and Prepare

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
• Form response team. • Manage security awareness across the organisation. • Implement cyber-safeguards that promote business continuity.	• Monitor security systems. • Detect cyber-incidents.	• Assess the severity of the incident. • Prioritise your response.	• Contain the incident. • Neutralise any threats. • Analyse.	• Document lessons learned.

The initial phase of cyber-continuity and incident response plans is all about groundwork. In this phase, you will want to form a response team, manage security awareness across your organisation and implement cyber-safeguards that promote business continuity. The following are key activities during Phase 1:

- Obtain management support, outlining the importance of cyber-continuity and incident response plans.
- Establish a cyber-continuity and incident response plan and policy that:
    - Describes which types of events should be considered incident
    - Establishes the organisational structure for incident response
    - Defines roles and responsibilities

  - Defines regulatory requirements

- Develop incident response procedures. These procedures should be detailed and outline steps for responding to a variety of cyber-incidents. They should cover every phase of the cyber-continuity and incident response plan and be based off a cyber-incident management policy. While specific response procedures will differ from organisation to organisation, they should account for:
  - Identifying and containing a breach
  - Recording information on the breach
  - Notifying key stakeholders, including employees, partners and customers
  - Training employees
- Inventory the data assets your organisation controls. Leadership should have an understanding of what kinds of losses would occur in the event of a breach. Identifying critical assets, quantifying potential losses and prioritising data can go a long way towards securing buy-in from upper management. Data should be prioritised based on its sensitivity and how important it is for daily operations. Specifically, when inventorying data, you should specify:
  - Who owns a particular set of data
  - Where the data is stored
  - What controls you have in place to safeguard your data
- Implement cyber-safeguards that promote business continuity. These controls should help your organisation successfully continue key operations and procedures in the event of a cyber-incident. Recommended continuity safeguards include:
  - Identify all critical financial and informational assets within your organisation, as well as key business operations for an accurate depiction of what your company needs to ensure continuity.
  - Create a list of emergency contacts and support services to rely on for continuity concerns in the event of a cyber-incident. This could include IT professionals, security consultants, technology service providers or web designers that help your organisation continue performing critical operations.
  - Define all back-up procedures and services necessary to protect your organisational assets and ensure continued operations. This could include having a back-up server for your business website to keep it active, alternative data accessibility options and controls that allow your company to continue taking online payments.
  - Train all staff members on your cyber-continuity practices, and ensure they understand their role in helping the businesses maintain operations during a breach.
  - Ensure proper communication with all partners, suppliers, clients and customers so they can be made aware of any cyber-concerns and important mitigation plans. This could entail establishing agreements with partners and suppliers for back-up operational procedures or data storage methods during a breach, as well as sharing alternative servicing options for clients or customers.

  - Work with your IT department to maintain updated, secure technology within your organisation. This includes proper malware and virus protection, routinely updated software, a secure internet connection and virtual private network (VPN), appropriate password protection and effective data encryption practices. Also, establish a continuity procedure for all technology that offers back-up data storage options.
  - Above all, make sure your organisation possesses robust cover that protects them from businesses interruption or continuity concerns resulting from cyber-attacks.

- Create a cyber-continuity and incident response team. Cyber-continuity and incident response plans must identify key internal and external personnel who are responsible for addressing a breach. Your incident response plan should outline the roles and responsibilities of these individuals and identify the procedures they must follow after a data incident. Be sure to account for all aspects of a data incident response, including planning, detecting and reporting, assessing, responding and post-incident review.

  The actual members of the team will vary depending upon the organisation and the nature of the incident. For example, smaller organisations may combine several responsibilities into one job role or outsource cyber-tasks altogether. In either case, the following areas must be accounted for when it comes to cyber-incident response:

  - Legal personnel
  - Public relations professionals
  - Customer care professionals
  - Corporate security officers
  - IT specialists

- Conduct training for team members.
- Develop a communications plan and awareness training for the entire organisation.
- Provide easy reporting mechanisms.
- Deploy endpoint security controls (e.g., anti-malware scanners) on information systems.
- Ensure that anti-malware scanners and other endpoint controls are updated frequently. Subscription-based security services should be renewed on a yearly basis. Once you let the subscription lapse, your information systems will immediately become vulnerable to cyber-threats.
- Establish relationships with governmental entities and local authorities.
- Practise your incident response plan capability, and assess continuity capabilities with penetration testing. This includes testing your organisation's plan by simulating common cyber-attack scenarios (eg malware infection, hacker infiltration, insider incident, network failure or denial of service) and looking for any concerns or vulnerabilities. A proper penetration test will help you understand the remaining risks present within your continuity and response plan, giving you the opportunity to fill any gaps and fix mistakes before a real incident occurs. Your test should follow these requirements:

  - Establish clear boundaries for the test, including the scenario(s) taking place, the general timeframe, the staff members involved and location(s) of the test.
  - Ensure your test meets all applicable legislative and reporting standards.
  - Identify any resources needed to complete the test, such as creating test accounts or allocating specific technology for the simulation.
  - Conduct a proper test report after the simulation has ended that includes an evaluation of how successful the existing plan was, security issues found, levels of risk or vulnerability present, and suggestions for improving the plan.

- **Involve competent legal advice or legal opinion.** To ensure effective plans, you should involve competent legal advice or legal opinion throughout the entire cyber-incident response process. Additionally, response plans should be consistent with applicable laws in relevant jurisdictions (e.g., jurisdictions where your organisation and customers are located).

Above all, you must make sure that your cyber-security plan is actionable and practicable. Cyber-continuity and incident response plans should be short, simple documents that:

- Specify tasks and outcomes.
- Assign accountability to specific incident response team members.
- Provide guidance and advice to help the incident response team make important technical, business and legal decisions in a timely manner.

Phase 2: Detect and Report

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
• Form response team. • Manage security awareness across the organisation. • Implement cyber-safeguards that promote business continuity.	• Monitor security systems. • Detect cyber-incidents.	• Assess the severity of the incident. • Prioritise your response.	• Contain the incident. • Neutralise any threats. • Analyse.	• Document lessons learned.

Phase 2 of cyber-continuity and incident response plans is dedicated to monitoring your organisation's IT systems. When it comes to responding to a threat, the quicker you act, the better.

With each day that passes after a cyber-incident, organisations accumulate more financial and reputational damage, making active monitoring a must. Specifically, the following are key activities to engage in during Phase 2:

- Create a method for employees and other partners to report suspicious activity. Monitor these reports carefully.
- Ensure your IT security systems are equipped with active monitoring protocols, notifying you following the discovery of an issue. You should also establish a method for monitoring and responding to these notifications. Causes of cyber-security incidents can vary, but are often the result of the following:
    - Attempts to gain unauthorised access to a system or its data
    - Attempts to disrupt an organisation's service delivery
    - Unauthorised access to information systems
    - Unauthorised changes to information systems
    - Malware infections
    - Malicious employees
    - Phishing emails and other spam
    - Infected USB flash drives
    - Malicious websites
    - The theft or loss of a laptop or smartphone
- Monitor information on potential and current cyber-threats shared by peers, government officials, suppliers and organisations who specialise in cyber-security, like the ICO.
- Look for signs of abnormal network activity. Signs that an IT infrastructure or system has been compromised can include, but are not limited to, the following:
    - Accounts or passwords no longer work
    - Company websites contain unauthorised changes
    - Computer systems run out of disk space or memory unexpectedly
    - You can no longer connect to your network
    - Computers crash constantly or reboot unexpectedly
    - Web browsers and other applications no longer function as expected
    - Your email contacts are receiving spam messages
    - Endpoint security controls, such as virus scanners, are no longer functioning
    - Your virus scanners or other security protocols inform you that an attempt has been made to compromise your network
    - System logs show suspicious activity

- **Gather relevant information, continue monitoring and detection practices**, and ensure reports are forwarded to your incident response team.

There are a variety of incident types, and your organisation should have a system in place to detect these threats. The chart below outlines various types of incidents.

TYPE	DESCRIPTION
Unauthorised access or usage	An individual gains access to a network, system or data without permission.
Service interruption or denial of service	An attack prevents access to a service or otherwise affects normal operation.
Malicious code	Malicious software like viruses, worms and Trojans are installed.
Network system failures (widespread)	Any incident that negatively affects the confidentiality, integrity or availability of a network.
Application system failures	Any incident that negatively affects the confidentiality, integrity or availability of an application.
Unauthorised disclosure or loss of information	Any incident that negatively affects the confidentiality, integrity or availability of data.
Privacy breach	Any incident that involves the real or suspected loss of personal information.
Information security/data breach	Any incident that involves the real or suspected loss of sensitive information.
Other	Any other incident that affects networks, systems or data.

Phase 3: Assess and Decide

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
• Form response team. • Manage security awareness across the organisation. • Implement cyber-safeguards that promote business continuity.	• Monitor security systems. • Detect cyber-incidents.	• Assess the severity of the incident. • Prioritise your response.	• Contain the incident. • Neutralise any threats. • Inform the ICO within 72 hours of the initial incident. • Analyse.	• Document lessons learned.

Suspicious network activity doesn't necessarily mean a cyber-event has occurred. Phase 3 of cyber-continuity and incident response involves assessing all cyber-events and determining responses accordingly. This phase occurs when initial signs of a breach occur and the response team must determine the scope of the attack. Specifically, the following are key activities to engage in during Phase 3:

- Assign a person from your incident response team to oversee the assessment of events.
- Determine, with the help of IT and other professionals, whether an event is actually a cyber-security concern or simply a false alarm. If you determine a cyber-security incident has occurred, escalate the event to the rest of your response team.
- Find out what information, system or network is affected by the event. Analyse the impact in terms of data confidentiality, integrity and priority.
- Notify the ICO within 72 hours of the initial incident. This is critical to avoid hefty fines.
- Find out if your business partners are affected.

When to Escalate an Incident

It is important for your employees to know when and how to report suspicious activities. While it may seem like certain scenarios do not need to be escalated up to an organisation's incident response team, employees should be trained to be overly cautious. At a minimum, employees should inform their manager or an IT team member of suspicious issues. The chart below outlines basic scenarios where issues should be reported:

EVENTS THAT SHOULD BE REPORTED TO INCIDENT RESPONSE TEAMS
• Suspicious emails with attachments or links
• Data breaches
• Theft or loss of your organisation's electronic devices (e.g., laptops and smartphones)
• Infections from viruses or other malicious software
• Denial-of-service attacks
• Suspicious or unauthorised network activity
• Third-party system, service or network failure
• The defacement or compromise of your organisation's online presence

Response Levels

In terms of responding to cyber-incidents, it's a good idea to organise threats in levels. These response levels will provide general guidance on the level of co-ordination required to respond to any given event. These levels may differ depending on the complexity of your operations and the data you store.

—	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
No cyber-security incidents have occurred. Critical and non-critical business functions are operating as normal.	No critical business functions are processed through the affected system. Malware (or some other malicious software) causes very little or no disruption in service delivery.	A small number of the organisation's critical business functions are processed through the affected system. Malicious software causes a minor disruption in service delivery depending on the system(s) impacted.	The majority of the organisation's critical business functions are processed through affected system. Malicious software causes a major disruption in service delivery depending on the system(s) impacted.	All of the organisation's critical business functions are processed through the affected system. Malware (or some other malicious software) causes a data breach or data destruction.

Phase 4: Respond

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
• Form response team. • Manage security awareness across the organisation. • Implement cyber-safeguards that promote business continuity.	• Monitor security systems. • Detect cyber-incidents.	• Assess the severity of the incident. • Prioritise your response.	• Contain the incident. • Neutralise any threats. • Inform the ICO within 72 hours of the initial incident. • Analyse.	• Document lessons learned.

Once you have determined the presence and severity of a threat, your organisation must respond accordingly. Response procedures allow organisations to contain a breach, investigate it and resolve the threat. While specific activities will differ depending on the type of attack, the following are key activities to engage in during Phase 4:

- Identify internal and external resources to help your organisation respond to the incident.
- Contain the problem, for example, by shutting down the system. For more specifics on containing incidents, click here.
- Remove the malicious components of the incident. For example, you could delete malware or disable a breached account.
- Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents.
- Conduct a forensic analysis of the incident, if applicable. To learn more about this step, click here.
- Notify the ICO within 72 hours of the initial incident. This is critical to avoid hefty fines.

Types of Incident Response

Responding to a cyber-incident can be a complex process—one that involves members from across your organisation. During Phase 4, consider the following types of responses to a cyber-incident:

1. Technical response—The technical response side of Phase 4 focuses on the actions of IT and other cyber-security personnel. Specifically, technical response teams are the individuals needed to resolve a specific cyber-threat. Technical response may involve several groups or departments, as containing, resolving, mitigating and repairing threats can be complex. Following a data breach, technical response is critical for restoring your systems to a healthy state. Whether your company has an in-house, technical-response capability or outsources it completely, your team should take proactive steps to protect your IT infrastructure.
2. Management response—Management response is any activity that requires high-level intervention, notification, interaction, escalation or approval. This can include things like co-ordinating internal and external communications, handling finances, ordering audits and overseeing regulatory compliance. For smaller organisations, management personnel are tasked with co-ordinating with third parties to ensure cyber-continuity and incident response initiatives are carried out properly.
3. Communications response—Communicating cyber-security incidents effectively can make a major difference when minimising reputational harm. These activities should involve senior leadership, DPOs or IT professionals, legal personnel, marketing, your cyber-continuity and incident response team and the ICO. Most importantly, every organisation should have a predetermined point of contact with the media, like a public relations expert trained on developing precise and impactful press releases. Your public relations expert should have communication templates ready to address different breach scenarios. Above all, communications response staff will need to balance the company's business interests with public transparency.
4. Legal response—When it comes to cyber-incident response, you should involve competent legal advice or legal opinion whenever possible. These individuals can provide advice and work with outside regulators, third parties and other stakeholders to manage any litigation concerns. In addition, you may want legal input for any external communications to guarantee compliance with company policies and regulatory requirements. Legal personnel should effectively act as quality control, reviewing everything from your mission statement to the response plan itself. Overall, legal experts ensure your firm exercises due care at all times, particularly when it comes to handling confidential information, evidence and documentation. In doing so, they proactively defend the organisation against liabilities. Legal aid is critical in the process of informing the ICO of a data breach.

Phase 5: Perform Post-incident Activities

PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
• Form response team. • Manage security awareness across the organisation. • Implement cyber-safeguards that promote business continuity.	• Monitor security systems. • Detect cyber-incidents.	• Assess the severity of the incident. • Prioritise your response.	• Contain the incident. • Neutralise any threats. • Inform the ICO within 72 hours of the initial incident. • Analyse.	• Document lessons learned.

Phase 5 outlines post-incident activities your organisation must complete following an incident. Again, this will differ based on the location of the organisation, the scope of the incident and the type of data affected by the breach. Phase 5 helps organisations learn from specific incidents and make key changes to improve cyber-security and the response process.

Specifically, the following are key activities to engage in during Phase 5:

- Identify the lessons learned from the cyber-security incident.
- Identify and make improvements to the organisation's security architecture.
- Review how effectively the incident response plan was executed during the cyber-security incident.

To aid in the recovery process of future incidents, organisations must evaluate the issues that caused the breach, how quickly they responded and how long the incident lasted. Effectively, during post-incident analysis, you must review and document everything that went well and poorly. The following are general questions to ask when evaluating incidents and your company's response practices:

1. What happened and at what time?
2. Was the incident found in a reasonable amount of time?
3. Was the system down longer than expected?
4. Were the right personnel available to respond? How well did staff and management perform in dealing with the incident?
5. Did recovery and restoration happen as quickly as expected?
6. Were backup files available and as up to date as possible?
7. Were documented procedures followed?

8. Were any steps or actions taken that might have inhibited the recovery?
9. What would staff and management do differently the next time a similar incident occurs?
10. What corrective actions can prevent similar incidents in the future? What additional tools or resources are needed to detect, analyse and mitigate future incidents?

After your assessment is complete, update and enhance your incident response plan. Auditing your plan helps make sure you're carrying out future response practices based on accurate and current information. In addition, assessing your plan helps you identify potential issues in advance and, should a future breach occur, ensures smoother response processes.

Regulatory Considerations

A major consideration to keep in mind throughout all phases of your cyber-continuity and incident response plan is regulatory compliance. Depending on where your business is located and what industry you operate in, a variety of specific data breach notification and reporting requirements may apply. Complicating the issue, it's an organisation's job to be informed on these different requirements. While regulatory bodies can provide general guidance, it's ultimately up to the business to implement compliance practices.

For UK organisations, there are two major compliance considerations to remember:

1. The GDPR
2. Payment card industry compliance

GDPR Compliance

Another major component of post-incident response is ensuring your organisation is compliant with UK data protection laws. The GDPR is legislation that guides businesses affected by data breaches.

Simply put, the GDPR creates strict requirements that force businesses to rethink their data security practices. The GDPR requires organisations to maintain records of all data breaches, report all data breaches to the ICO and disclose harmful data breaches to affected individuals. In addition, the GDPR requires organisations to have a lawful basis for gathering, processing and holding data on individuals in the first place, providing individuals with the right to know how their data is being used and the right to request their data be removed or erased.

These requirements, set forth by the ICO, are designed to keep UK citizens informed any time a data breach poses a threat to their personal information. The GDPR attempts to accomplish this goal by requiring organisations to do the following:

1. Submit a report to the ICO any time a data breach occurs. Complete this step within 72 hours of the breach occurrence.
2. Notify individuals any time there is a data breach that affects the individual's information and creates a significant risk of harm to the individual. Only collect data from an individual under a lawful basis, respond to subject access requests in a timely manner and allow individuals to 'opt-out' at any time, entailing data removal or erasure.
3. Maintain records of each data breach involving personal information under the organisation's control.

For an informative guide on specific GDPR requirements, contact Macbeth.

Payment Card Industry Compliance

To help protect customers, it's critical that any organisation that accepts payment cards understands the payment card industry's (PCI) Data Security Standards (DSS). The PCI DSS is a set of requirements designed to ensure that all entities that process, store or transmit credit card information maintain a secure environment. In essence, the PCI DSS establishes a minimum set of requirements for protecting the account information of cardholders. Regardless of whether a merchant processes one credit card a year or 1 million, they must adhere to the PCI DSS.

There are four major steps to compliance, as outlined by the PCI Security Standards Council. If followed closely, these steps can help merchants of any size integrate PCI DSS into their businesses. Those steps include the following:

1. Determine merchant level—This step involves determining which merchant level applies to your organisation as determined by the payment card brands you accept.
2. Assess—This process involves identifying vulnerabilities in your IT assets and payment card processing systems.
3. Remediate—After you have assessed all PCI DSS issues, you must fix any security vulnerabilities you have found.
4. Report—Once you have assessed and remediated vulnerabilities, you must document your compliance efforts and submit them to the acquirers and payment card companies you are working with.

Navigating the PCI DSS can be taxing for the average organisation, as an overview of PCI DSS compliance specifics and best practices are rarely found under one, all-encompassing source. Moreover, the PCI DSS itself is over 100 pages and is filled with acronyms and terminology that can be confusing. PCI DSS compliance is not something that can be easily addressed on your own—especially if you are a merchant with limited resources. Contact Macbeth for a general guide to PCI DSS compliance.

Executing the Plan

While having an understanding of the mechanics of a cyber-continuity and incident response plan is important, knowing how to effectively execute the plan is critical. When a cyber-attack occurs, it can be chaotic. Understanding how to use your plan can minimise the impact of an incident.

Contain the Incident

As part of Phase 4 of your incident response plan, containing threats quickly and thoroughly is essential for recovering from a breach. Following every incident, whether it's a data breach or the loss of physical assets (e.g., company laptops), you will need to make split-second decisions on how best to act. Immediately after the detection of an incident, consider the following:

1. Discovery—Record the date, time, location and duration of the breach. You will want to note whether this was a one-off incident or an attack that has been persistent for months. In addition, document who discovered the breach and how.
2. Breach—Document specifics regarding the breach. This can include details on:
    a. Point of entry
    b. Method of intrusion
    c. The systems affected
    d. What information was accessed, deleted, modified or taken
3. Data—Catalogue details regarding the data, including who was affected, where the affected individuals are located, what type of information was compromised and how many records were impacted.

To help you contain an incident, the following checklist outlines considerations to keep in mind:

CONTAINING THE INCIDENT	YES	NO	N/A
Have you limited employee and public access to the affected area? Have you changed locks, access card permissions and passwords?	☐	☐	☐
Have you notified the ICO, local authorities or other officials?	☐	☐	☐
Have you conducted an internal or external investigation? If so, have you identified any employee misconduct and notified HR?	☐	☐	☐
Have you determined what assets have been lost or affected?	☐	☐	☐
Did you record the date, time, location and duration of the breach? Did you record who discovered the breach and how?	☐	☐	☐
Did you determine whether this was a one-off incident or persistent event?	☐	☐	☐
Did you document details on point of entry, method of intrusion, the systems affected and what information was accessed, deleted, modified or taken?	☐	☐	☐
Did you catalogue details regarding the data, including who was affected, where the affected initials are located, what type of information was compromised and how many records were impacted?	☐	☐	☒

Convene Your Cyber-continuity and Incident Response Team

Once you have determined a cyber-event should be reported to your response team, you will have to escalate the incident and convene the team itself.

Team members should be assembled and briefed. If possible, communications between team members should be done by phone only to avoid using potentially compromised email systems. The actual members of the team will vary depending upon the organisation and the nature of the incident. However, team member responsibilities generally cover the following areas:

LEGAL/COMPLIANCE	PUBLIC RELATIONS/MARKETING	CUSTOMER CARE DEPARTMENT	HUMAN RESOURCES	CORPORATE SECURITY AND IT
• Implements a privilege protocol • Determines how to notify affected individuals, the media, police, ICO and other third parties • Establishes and manages relationships with outside counsel before an incident • Manages communications with privacy commissioners and regulators • Ensures internal documents and reports are generated at the counsel's direction • Issues and monitors a litigation hold • Reviews all outgoing communications, filings, reports, etc.	• Identifies key media and crisis-response strategies • Executes an internal communication plan that addresses confidentiality and appropriate employee actions • Tracks and analyses media coverage, responding to negative coverage if necessary	• Determines whether incident inquiries will be dealt with internally or whether a call centre will be utilised • Sets up a call centre and consumer protection programme to handle customer complaints	• Manages employees during the incident, shifting employee resources as required • Handles internal investigations, disciplinary actions and terminations if the incident is the result of employee wrongdoing	• Communicates with police (alongside the legal team) • Manages incident risks as well as the isolation of affected areas • Works alongside external IT forensics professionals to identify and remove any malicious code or other remnants of a data incident • Assists with evidence gathering and litigation efforts

Analyse the Incident

The moment an incident is identified, you should begin gathering and analysing the information available. Notably, any information you gather is subject to a comprehensive litigation hold. Therefore, this data must be preserved, collected and analysed at the direction of counsel (and provided to police if required/appropriate). Your legal team can help you review any information gathered to determine if it is relevant.

Following a data breach or other incident, your organisation has a very short window to collect key evidence. While your IT team will essentially act as a first responder, they may not have the necessary training to conduct data recovery and analysis procedures. Because of this, outside IT forensics teams specialising in data breach response should be retained.

These firms should be able to:

- Identify and neutralise threats.
- Preserve and manage evidence using data recovery tools and processes.
- Work across various operating systems and devices.
- Manage forensic practices in a way that respects employee sensitivities and workplace culture.
- Identify individuals who can provide testimony and appear as confident witnesses in court.
- Understand privilege issues, litigation holds and the role their firm plays in regulatory and court proceedings.

Organisations should establish relationships with experienced forensics firms long before a breach ever occurs.

Be Prepared, Remain Protected

While organisations may take every necessary precaution, they are seldom prepared for a major cyber-security event. These events can put a serious strain on finances, resources, technology and reputations, particularly if you fail to create an effective cyber-continuity and incident response plan.

These plans, alongside cyber-security programmes and cyber-liability insurance, decrease the likelihood that your organisation will close as the result of an attack. It should be noted that there is no agreed-upon format for cyber-continuity and incident response plans, but many do share commonalities. To review a sample plan and begin the process of creating one of your own, look to the next section of this toolkit.

To learn more about basic cyber-security protections and cover options, contact us today. We will be able to assist you with all of your cyber-risk management needs, providing insight into the steps you need to take to better protect your business.

SAMPLE CYBER-CONTINUITY AND INCIDENT RESPONSE PLAN

CYBER-CONTINUITY AND INCIDENT RESPONSE PLAN

Organisation name:

Review cycle:

Address:

Prepared by:

Date:

This cyber-continuity and incident response plan ensures that is prepared to respond to a variety of threats in an effective and efficient manner. Working alongside ’s Data Breach Response Policy, this plan documents the roles, responsibilities and steps that will be followed to identify, contain, eradicate and recover from cyber-security incidents. By having a plan, a team and conducting exercises, organisations will be better prepared for inevitable incidents and will be able to contain the damage, allow for continued operations and mitigate further risk to the organisation.

This plan applies to all networks, systems and data as well as employees, contractors and suppliers that access these systems.

Revision History

This cyber-continuity and incident response plan has been modified as follows:

DATE	VERSION	DESCRIPTION OF THE MODIFICATION	MODIFIER

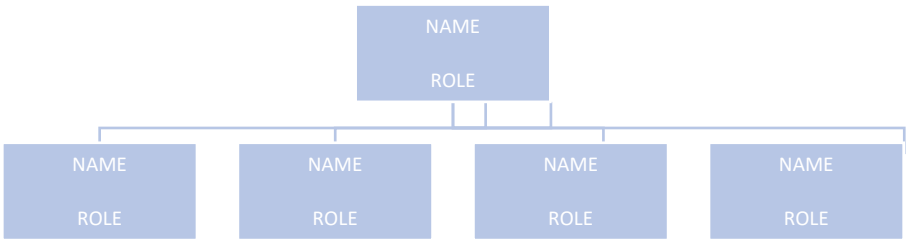
Roles and Responsibilities

INTERNAL CONTACTS				
TITLE	NAME	RESPONSIBILITIES	PHONE	EMAIL
CEO or other company leader				
DPO or other high-ranking IT professional				
Human resources manager				
Customer care manager				
Marketing and public relations manager				

Legal representative				

EXTERNAL CONTACTS				
TYPE	ROLE	COMPANY NAME	PHONE	EMAIL
Supplier	Service provider			
Supplier	Forensics team on retainer			
Supplier	Technology supplier			
Connected organisation	Peer			

Incident Response Team Structure*



**To add more roles to this flow chart, click into the image, then double-click on a specific box. From there, use the "subordinate" and "assistant" buttons located at the far left of the document ribbon.*

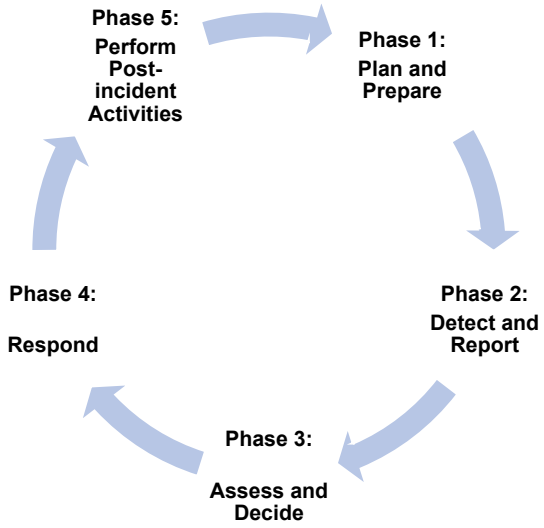
Incident Types and Escalation

One of the major roles of the incident response team is to assess the various incidents reported to them by employees or antivirus software and similar protections. If an incident is determined to be a threat, the team will prioritise the response process based on the escalation level. The charts below outline common incident types and various threat levels.

TYPE	DESCRIPTION
Unauthorised access or usage	An individual gains access to a network, system or data without permission.
Service interruption or denial of service	An attack prevents access to a service or otherwise affects normal operation.
Malicious code	Malicious software like viruses, worms and Trojans are installed.
Network system failures (widespread)	Any incident that negatively affects the confidentiality, integrity or availability of a network.
Application system failures	Any incident that negatively affects the confidentiality, integrity or availability of an application.
Unauthorised disclosure or loss of information	Any incident that negatively affects the confidentiality, integrity or availability of data.
Privacy breach	Any incident that involves the real or suspected loss of personal information.
Information security/data breach	Any incident that involves the real or suspected loss of sensitive information.
Other	Any other incident that affects networks, systems or data.

—	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
No cyber-security incidents have occurred. Critical and non-critical business functions are operating as normal.	No critical business functions are processed through the affected system. Malware (or some other malicious software) causes very little or no disruption in service delivery.	A small number of the organisation's critical business functions are processed through the affected system. Malware (or some other malicious software) causes a minor disruption in service delivery depending on the system(s) impacted.	The majority of the organisation's critical business functions are processed through affected system. Malware (or some other malicious software) causes a major disruption in service delivery depending on the system(s) impacted.	All of the organisation's critical business functions are processed through the affected system. Malware (or some other malicious software) causes a data breach or data destruction.

Incident Handling



PHASE 1: PLAN AND PREPARE	PHASE 2: DETECT AND REPORT	PHASE 3: ASSESS AND DECIDE	PHASE 4: RESPOND	PHASE 5: PERFORM POST-INCIDENT ACTIVITIES
• Form response team. • Manage security awareness	• Monitor security systems. • Detect cyber-incidents.	• Assess the severity of the incident. • Prioritise your response.	• Contain the incident. • Neutralise any threats. • Inform the ICO within 72 hours of the incident.	• Document lessons learned.

across the organisation. • Implement cyber-safeguards that promote business continuity.			• Analyse.	

Plan and Prepare

ITEM	
Obtain support from board members or other executives, outlining the importance of cyber-continuity and incident response plans.	☐
Establish a cyber-continuity and incident management policy that: • Describes which types of events should be considered incident • Establishes the organisational structure for incident response • Defines roles and responsibilities • Defines regulatory requirements	☐
Develop incident response procedures. These procedures should be detailed and outline steps for responding to a variety of cyber-incidents. They should also cover every phase of the cyber-continuity and incident response plan and be based off an overall cyber-continuity and incident management policy. While specific response procedures will differ from organisation to organisation, they should account for: • Identifying and containing a breach • Recording information on the breach and reporting it to the ICO • Notifying key stakeholders, including employees, partners and customers • Training employees	☐
Inventory the data assets your organisation is responsible for. Leadership should have an understanding of what kinds of losses would occur in the event of a breach. Identifying critical assets, quantifying potential losses and prioritising data can go a long way towards securing buy-in from upper management and a cyber-security budget. This data should be prioritised based on its sensitivity and how important it is for daily operations. Specifically, when inventorying data, you should specify: • Who owns a particular set of data • Where the data is stored • What controls you have in place to safeguard your data	☐
Implement cyber-safeguards that promote business continuity. These controls should help your organisation successfully continue key operations and procedures in the event of a cyber-incident. Recommended continuity safeguards include: • Identify all critical financial and informational assets within your organisation, as well as key business operations for an accurate depiction of what your company needs to ensure continuity. • Create a list of emergency contacts and support services to rely on for continuity concerns in the event of a cyber-incident.	☐

• Define all back-up procedures and services necessary to protect your organisational assets and ensure continued operations. • Train all staff members on your cyber-continuity practices, and ensure they understand their role in helping the businesses maintain operations during a breach. • Ensure proper communication with all partners, suppliers, clients and customers so they can be made aware of any cyber-concerns and important mitigation plans. • Work with your IT department to maintain updated, secure technology within your organisation. • Make sure your organisation possesses robust cover that protects them from businesses interruption or continuity concerns resulting from cyber-attack.	
Create a cyber-continuity and incident response team. Cyber-continuity and incident response plans must identify key internal and external personnel who are responsible for addressing a breach. You incident response plan should outline the roles and responsibilities of these individuals and outline the procedures they must follow after a data incident. Be sure to account for all aspects of a data incident response, including planning, detecting and reporting, assessing, responding and post-incident review. The actual members of the team will vary depending upon the organisation and the nature of the incident, but generally account for the following areas: • Legal personnel • Public relations professionals • Customer care professionals • Corporate security officers • IT specialists and the DPO	☐
Conduct training for team members.	☐
Develop a communications plan and awareness training for the entire organisation.	☐
Provide easy reporting mechanisms.	☐
Deploy endpoint security controls (e.g., anti-malware scanners) on information systems.	☐
Ensure that anti-malware scanners and other endpoint controls have their databases updated frequently. Subscription-based security services, such as anti-malware software, typically must be renewed on a yearly basis. Once you let the subscription lapse, your information systems will immediately become vulnerable to cyber-threats.	☐
Establish relationships with the ICO and local authorities.	☐
Practise your incident response plan and continuity capabilities with penetration testing.	☐
Involve competent legal advice or legal opinion. To ensure effective plans, you should involve a legal team throughout the entire cyber-continuity and incident response process. Additionally, response plans should be consistent with applicable laws in relevant jurisdictions.	☐

Detect and Report

ITEM	
Create a method for employees and other partners to report suspicious activity. Monitor these reports carefully.	☐
Ensure your IT security systems are equipped with active monitoring protocols, notifying you following the discovery of an issue. You should also establish a method for monitoring and responding to these notifications.	☐

Monitor information on potential and current cyber-threats shared by peers, officials, suppliers and organisations who specialise in cyber-security, like the ICO.	☐
Look for signs of abnormal network activity.	☐
Gather relevant information, continue monitoring and detection practices, and send reports to your incident response team.	☐

Assess and Decide

ITEM	
Assign a person from your incident response team to oversee the assessment of a particular event.	☐
Determine, with the help of IT and other professionals, whether an event is actually a cyber-security concern or simply a false alarm. If you determine a cyber-security incident has occurred, escalate the event to the rest of your response team.	☐
Find out what information, system or network is affected by the event. Analyse the impact in terms of data confidentiality, integrity and priority.	☐
Notify the appropriate officials.	☐
Find out if your business partners are affected.	☐
Use your incident identification and escalation charts to prioritise any incidents.	☐

Respond

ITEM	
Identify internal and external resources to help your organisation respond to the incident.	☐
Contain the problem, for example, by shutting down the system.	☐
Remove the malicious components of the incident. As an example, you could delete malware or disable a breached account.	☐
Recover from the incident by restoring systems to normal operation and fixing the vulnerabilities to prevent similar incidents.	☐
Conduct a forensic analysis of the incident, if applicable.	☐

Perform Post-incident Activities

ITEM	
Identify the lessons learned from the cyber-security incident.	☐
Identify and make improvements to the organisation’s security architecture.	☐
Review how effectively the incident response plan was executed during the cyber-security incident.	☐

APPENDIX: SAMPLE CYBER-SECURITY DOCUMENTS

CYBER RISK EXPOSURE CALCULATOR

In recent years, cyber-attacks have emerged as one of the most significant threats facing organisations of all sizes. The internet and other network operations have created risks that were non-existent less than a decade ago. When cyber-attacks (such as data breaches and hacks) occur, they can result in devastating damage, such as business disruptions, revenue loss, legal fees, a permanently tainted reputation, and more.

It is important to remember that no organisation is immune to the impact of cyber-crime. As a result, cyber-liability insurance has become an essential component to any risk management programme.

Instructions: Begin by answering the questions below. Each response will be given a numerical value depending on the answer:

- YES: 5 points **- NO:** 0 points **- UNSURE:** 5 points

After completing all of the questions, total your score to determine your organisation's level of cyber risk using the scale below.

EXPOSURE	YES	NO	UNSURE	SCORE
1. Does your organisation have a wireless network, or do employees or customers access your internal systems from remote locations?	☐	☐	☐	
2. Does anyone in your organisation take company-owned mobile devices (eg, laptops, smart-phones and USB drives) with them, either home or when travelling?	☐	☐	☐	
3. Does your organisation use Cloud-based software or storage?	☐	☐	☐	
4. Does your organisation have a 'bring your own device' (BYOD) policy that allows employees to use personal devices for business use or on a company network?	☐	☐	☐	
5. Are any employees allowed access to administrative privileges on your network or comput-ers?	☐	☐	☐	
6. Does your organisation have critical operational systems connected to a public network?	☐	☐	☐	
7. Does anyone in your organisation use computers to access bank accounts or initiate money transfers?	☐	☐	☐	
8. Does your organisation store sensitive information (eg, financial reports, trade secrets, intel-lectual property and product designs) that could potentially compromise your organisation if stolen?	☐	☐	☐	
9. Does your organisation digitally store sensitive employees' or customers' sensitive informa-tion? This can include government-issued ID numbers and financial information.	☐	☐	☐	
10. Is your organisation part of a supply chain, or do you have supply chain partners?	☐	☐	☐	
11. Does your organisation conduct business in foreign countries, either physically or on-line?	☐	☐	☐	
12. Has your organisation ever failed to enforce policies around the acceptable use of comput-ers, email, the Internet, etc?	☐	☐	☐	
13. Can the general public access your organisation's building without the use of an ID card?	☐	☐	☐	
14. Is network security training for employees optional at your organisation?	☐	☐	☐	
15. Can employees use their computers or company-issued devices indefinitely without updat-ing passwords?	☐	☐	☐	
16. Has your IT department ever failed to install antivirus software or perform regular vulnera-bility checks?	☐	☐	☐	
17. Can employees dispose of sensitive information in unsecured bins?	☐	☐	☐	
18. Would your organisation lose critical information in the event of a system failure or other network disaster?	☐	☐	☐	
19. Can employees easily see what co-workers are doing on their computers?	☐	☐	☐	
20. Has your organisation neglected to review its data security or cyber security policies and procedures within the last year?	☐	☐	☐	
TOTAL SCORE:				

Escalated Risk: 55-100 | **High Risk:** 30-50 | **Moderate Risk:** 15-25 | **Low Risk:** 0-10

CHECKLIST | PERSONAL DATA BREACHES UNDER THE GDPR

Presented by Macbeth

The UK General Data Protection Regulation (UK GDPR) introduced a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

A personal data breach refers to a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In 2021, 4 in 10 businesses (39 per cent) and a quarter of charities (26 per cent) reported cyber-security breaches or attacks within the last 12 months.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform those individuals without undue delay. You should ensure that you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Under the GDPR, an organisation may be fined up to £17.5 million or 4 per cent of its annual turnover—whichever is higher—for violating the basic principles related to data security. What's more, if your organisation fails to notify the relevant supervisory authority of a breach, it can result in a fine of up to £8.7 million or 2 per cent of your annual turnover, depending on which is higher.

Use this checklist to comply with the GDPR's rules surrounding personal data breaches:

PREPARING FOR A DATA BREACH	YES	NO	ADDITIONAL NOTES
We know how to recognise a personal data breach.	☐	☐	
We understand that a personal data breach isn't only about loss or theft of personal data.	☐	☐	
We have prepared a response plan for addressing any personal data breaches that occur.	☐	☐	
We have allocated responsibility for managing breaches to a dedicated person or team.	☐	☐	
Our staff knows how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.	☐	☐	

CHECKLIST | PERSONAL DATA BREACHES UNDER THE GDPR

RESPONDING TO A DATA BREACH	YES	NO	ADDITIONAL NOTES
We have in place a process to assess the likely risk to individuals as a result of a breach.	☐	☐	
We know who is the relevant supervisory authority for our processing activities.	☐	☐	
We have a process to notify the Information Commissioner's Office (ICO) of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.	☐	☐	
We know what information we must give the ICO about a breach.	☐	☐	
We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.	☐	☐	
We know we must inform affected individuals without undue delay.	☐	☐	
We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.	☐	☐	
We document all breaches, even if they don't all need to be reported.	☐	☐	

HOW TO REPORT A DATA BREACH	COMPLETED
Contact the relevant supervisory authority of a breach within 72 hours of your organisation becoming aware of it.	☐
Directly contact individuals affected by a breach if it is likely to result in a high risk to their rights and freedoms. (Note: A 'high risk' means the threshold for notifying individuals is greater than notifying the relevant supervisory authority.)	☐
Complete a breach notification, which should contain the following information: • The categories and number of individuals affected by the breach • The categories and number of personal data records affected by the breach • The name and contact details of the data protection officer (if your organisation has one) or an additional contact where more information can be obtained • A detailed description of the potential consequences of the data breach • A detailed description of what measures your organisation has taken or will take to address the data breach • A detailed description of the measures your organisation has taken or will take to mitigate any possible adverse effects to either itself or the individuals affected	☐

POLICY

Data Breach Response

Location: [INSERT LOCATION]

Effective Date: [INSERT DATE]

Revision Number: [INSERT #]

PURPOSE

This policy establishes how will respond in the event of a data breach, and also outlines an action plan that will be used to investigate potential breaches and to mitigate damage if a breach occurs. This policy is in place to both minimise potential damages that could result from a data breach and to ensure that parties affected by a data breach are properly informed of how to protect themselves.

SCOPE

This policy applies to all incidents where a breach of customer or employee personal identifying information is suspected or confirmed.

DEFINITIONS

Personal data (PD) – Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. PD includes, but is not limited to, any of the following:

- Credit card information (eg credit card numbers – whole or part, credit card expiry dates, cardholder names, cardholder addresses)
- VAT identification numbers, business identification numbers and employer identification numbers
- Biometric records (eg fingerprints, DNA, or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information (eg pay cheques or pay stubs)
- Medical information for any employee or customer (eg doctor names and claims, insurance claims, prescriptions or any related personal medical information)
- Other personal information of a customer, employee or contractor (eg dates of birth, addresses, phone numbers, maiden names, names or customer numbers)

Breach – Any situation where PD is accessed by someone other than an authorised user for anything other than an authorised purpose.

POLICY GUIDELINES

Upon Learning of a Breach

A breach or a suspected breach of PD must be immediately investigated. Since all PD is of a highly confidential nature, only personnel necessary for the data breach investigation will be informed of the breach. The following information must be reported to appropriate management personnel:

- When (date and time) did the breach happen?
- How did the breach happen?
- What types of PD were obtained? (As detailed as possible: name, account number, password, etc) How many customers were affected?

Management will then make a record of events and people involved, as well as any discoveries made over the course of the investigation and determine whether or not a breach has occurred.

Perform a Risk Assessment

Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the PD lost (customer contact information alone may present much less of a threat than financial information)
- Amount of PD lost and number of individuals affected

- Likelihood PD is usable or may cause harm
- Likelihood the PD was intentionally targeted (increases chance for fraudulent use)
- Strength and effectiveness of security technologies protecting PD (eg encrypted PD on a stolen laptop is technically stolen PD but with a greatly decreased chance of access)
- Ability of to mitigate the risk of harm

All information collected during the risk assessment must then be compiled into one report and analysed. The risk assessment must then be provided to appropriate personnel in charge of data breach response management. will keep a record of any personal data breach, regardless of whether there is a requirement to notify affected parties.

Notifying Affected Parties

Responsibility to notify is based both on the number of individuals affected and the nature of the PD that was accessed. Any information found in the initial risk assessment will be turned over to a competent legal professional of who will review the situation to determine if, and to what extent, notification is required.

Notification should occur in a manner that ensures the affected individuals will receive notice of the incident. Notification will be made in a timely manner, but not so soon as to unnecessarily compound the initial incident with incomplete facts or to make identity theft more likely through the notice. By law, will report certain types of types of data breach to the Information Commissioner's Office (or the appropriate supervisory authority) within 72 hours, where feasible. The 72-hour period begins once the organisation becomes aware of the breach.

In the case that notification must be made:

- Only those that are legally required to be notified will be informed of the breach. Notifying a broad base when it is not required could raise unnecessary concern in those who have not been affected.
- Individuals who are in a high risk to be adversely affected will be notified without undue delay.
- A physical copy will be posted to the affected parties no matter what other notification methods are used.
- A helpline will be established for those who have additional questions about how the breach with affect them.

The notification will include:

- A brief description of the incident, including (when possible):
    - The approximate date it occurred;
    - The categories and approximate number of individuals concerned; and
    - The categories and approximate number of personal data records concerned;
- A description of the type(s) of PD that were involved in the breach (the general types of PD, not an individual's specific information);
- A description of the likely consequences of the personal data breach;
- Explanation of what is doing to investigate the breach, mitigate its negative effects and prevent future incidences;
- Contact information for 's data protection officer (if applicable) or other contact point where more information can be obtained; and
- Steps the individual can take to mitigate any potential side effects from the breach.

Mitigating Risks

Based off the findings of the risk assessment, a plan will be developed to mitigate risk involved with the breach. The exact course of action will be based on the type of PD that was involved in the data breach. As with any security incident, you should investigate whether or not the breach was a result of human error or a system issue and see how a recurrence can be prevented—whether this is through better processes, further training or other corrective steps.

The course of action will aim to minimise the effect of the initial breach and to prevent similar breaches from taking place.

- Affected individuals will be notified as soon as possible so they can take their own steps to mitigate potential risk.
- If there is a substantial concern for fraudulent use of PD, will offer affected individuals free access to a credit monitoring service.

POLICY

General Email / Internet Security and Use

Location: [INSERT LOCATION]

Effective Date: [INSERT DATE]

Revision Number: [INSERT #]

GENERAL SECURITY POLICY

The General Email/Internet Security and Use Policy forms the foundation of the corporate Information Security Programme. Information security policies are the principles that direct managerial decision making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorised behaviour for personnel approved to use information assets.

Applicability

The General Email/Internet Security and Use Policy applies to all employees, interns, contractors, suppliers and anyone using assets. Policies are the organisational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks and components owned or leased by or its designated representatives.

General Policies

All employees, contractors, suppliers and any other person using or accessing information or information systems must adhere to the following policies.

- All information systems within are the property of and will be used in compliance with policy statements.
- Any personal information placed on information system resources becomes the property of .
- Any attempt to circumvent security policy statements and procedures (ie, disconnecting or tunnelling a protocol through a firewall) is strictly prohibited.
- Unauthorised use, destruction, modification and/or distribution of information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate policy statements prior to use of information assets and information systems.
- At a minimum, all users will be responsible for understanding and complying with the following policy statements:
    - General Security Policy
    - System Security Policy
    - Desktop Service Security Policy
    - Internet Acceptable Use Policy
    - Personal Equipment Policy
    - Virus, Hostile and Malicious Code Policy
- All users will report any irregularities found in information or information systems to the IT team immediately upon detection.
- information systems and information will be subject to monitoring at all times. Use of information systems constitutes acceptance of this monitoring policy.
- Use of any information system or dissemination of information in a manner bringing disrepute, damage or ill-will against is not authorised.
- Release of information will be in accordance with Policy Statements
- Users will not attach their own computer, test equipment or personal software (including software applications) to computers or networks without prior approval of the IT team or its designated representative.
- If a user fails to comply with this policy, he or she will face disciplinary proceedings, up to and including dismissal.

SYSTEM SECURITY POLICY

’s System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by .

Applicability

The System Security Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

Password System Security

In today’s information age, poorly selected, reusable passwords represent the most vulnerable aspects of information security. has adopted this policy to ensure that the private information of our clients and our proprietary corporate data are kept secure at all times. -authorised users must comply with creation, usage and storage policies to minimise risk to corporate information assets.

- Passwords will conform to the following criteria:
    - Passwords will be a minimum of [insert number] characters
    - Passwords must also contain [edit as needed, for example: at least one uppercase letter, one lowercase letter and one number].
- The sharing of passwords is prohibited.
- Any suspicious queries regarding passwords will be reported to the IT team.
- Passwords will be protected as proprietary information. Writing them down or storing them unencrypted on the information system is prohibited.
- Users will be forced to change passwords every [insert number] days and may reuse passwords only after [insert number] different passwords have been used.
- Accounts will be locked out after [insert number] failed password attempts in a [insert number]-minute time period. Accounts can be reset by contacting the IT team or by waiting [insert number] minutes for the account to reset automatically.
- Users will be forced to unlock their computers using their network password after [insert number] minutes of inactivity on their desktops.
- All system passwords will be changed within [insert number] hours after a possible compromise.
- When users leave the organisation, their accounts will be deleted.
- If the user leaving the organisation was a privileged user or a network administrator, all system passwords will be changed.

DESKTOP SERVICES SECURITY POLICY

The Desktop Services Security Policy addresses the authorised and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any information system.

- No software of any kind will be installed onto a laptop or desktop computer without the approval of the IT team.
- Only system administrators will have the ability to install software.
- Unauthorised copying or distributing of copyrighted software is a violation of UK Copyright Law and will not be permitted.
- Personal software (including software applications) will not be installed on any machine.
- Users will not allow non-employees to use any machine or device without authorisation of the IT team.
- The following items are corporate policy for security monitoring:
    - All systems and network activities will be subject to monitoring. Use of systems and networks constitutes consent to this monitoring.
    - Disabling or interfering with virus protection software is prohibited.
    - Disabling or interfering with logging, auditing or monitoring software is prohibited.
    - All desktop services will be subject to inventory and inspection.
    - Security irregularities, incidents, emergencies and disasters related to information or system will be reported to the IT team immediately.

- The following items are corporate policy for system usage:
    - Sabotage, destruction, misuse or unauthorised repairs are prohibited on information systems.
- All repairs will be authorised and performed by the IT team.
    - Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on the information system.
    - All data on information systems at is classified as company proprietary information.
    - Users will secure all printed material and other electronic media associated with their use of information and information systems.
    - Storage, development or the unauthorised use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

INTERNET ACCEPTABLE USE POLICY

Internet access is provided to employees to conduct business. While these resources are to be used primarily for business, the company realises that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

- Non-business internet activity will be restricted to non-business hours. actively blocks non-business sites during working hours. Working hours are defined as [insert working hours, for example: Monday – Friday from 7:00–12:00 and from 12:45–17:00 hours].
- The definition of non-business sites is the sole discretion of the IT team. This definition may change without notice as the internet continues to evolve.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a domain address (such as posting to newsgroups, use of chat facilities and participation in email lists) must not bring disrepute to or associate with controversial issues (ie, sexually explicit materials).
- Internet use must not have a negative effect on operations.
- Users will not make unauthorised purchases or business commitments through the internet.
- Internet services will not be used for personal gain.
- Internet users will make full attribution of sources for materials collected from the Internet. Plagiarism or violation of copyright is prohibited.
- Release of proprietary information to the internet (ie, posting information to a newsgroup) is prohibited.
- All internet users will immediately notify the IT team of any suspicious activity.
- All remote access to the internal network through the internet will be encrypted and authenticated in a manner authorised by the IT team.
- Accessing personal social networking accounts (including but not limited to Facebook®, Twitter®, Google+®, MySpace®, LinkedIn®, Foursquare® and TUMBLR®) or using email for personal social networking purposes is prohibited during working hours. The use of social networking sites for specific business purposes must be pre-approved or assigned by a manager/supervisor.

EMAIL SECURITY POLICY

The Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides representatives of in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Applicability

The Email Security Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

Policy

Authorised users are required to adhere to the following policies. Violators of any policy are subject to disciplinary actions, up to and including termination.

The following items are the corporate policy statements for Access Controls:

- All email on the information systems, including personal email, is the property of . As such, all email can and will be periodically monitored for compliance with this policy.
- Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members, such as between a producer and an account representative. In all other cases, no user is authorised to open or read the e-mail of another without the express consent of senior management.
- Email is provided to the users of primarily to enhance their ability to conduct business.
- Email will be stored on the system up to a maximum of [insert number] MB per mailbox. Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size reaches [insert number] MB. However, once the mailbox storage space exceeds [insert number] MB, users will not be able to send new messages until the mailbox size falls below the [insert number] MB limit. In all cases, however, users will continue to receive incoming messages.
- The maximum size of any individual incoming email message will be [insert number] MB.
- Terminated employees will have all email access immediately blocked.
- Users who leave the company will have all new e-mails automatically forwarded to their supervisor, or their designated representative, for [insert number] days.
- The former employee's supervisor is responsible for disseminating stored emails to the appropriate party. Thirty days after the date of termination, the former employee's mailbox will be permanently removed from the system.

The following items are the corporate policy statements for Content:

- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (ie, global send) is prohibited. This includes the forwarding of chain letters.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, colour, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (ie, identification, addresses) is prohibited.
- All outgoing email will automatically include the following statement: [insert company email confidentiality statement, for example: "This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer."]

The following items are the corporate policy statements for Usage:

- Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
- When sending email, users should verify all recipients to whom they are sending the message(s).
- Be aware that deleting an email message does not necessarily mean it has been deleted from the system.

PERSONAL EQUIPMENT POLICY

This policy provides guidelines for using corporate IT support resources for personally owned equipment and related software including, but not limited to: notebook computers, desktop computers, personal digital assistants (PDAs), smartphones and mobile phones.

Applicability

The Personal Equipment Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or his/her designated representative.

General Policy

 recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

- As a general rule, employees of will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

- Personally owned notebooks and desktop computers will not be granted direct physical access to the network. Employees that wish to access the network from a remote location using their personally owned computer may do so using only -authorised software and only with the approval of the employee's supervisor or manager.
- PDAs and smart phones, which include devices using BlackBerry®, iPhone®, Windows Mobile®, Android®, Linux® and Palm® technologies, will be supported according the following rules:
    - Employees are responsible for learning, administering, installing and setting up their own PDAs or smartphones.
    - Corporate IT resources should not be used for assistance in the basic operation of these devices.
    - Upon request, the IT team will install the necessary synchronisation software to the employee's desktop or notebook computer.

VIRUS, HOSTILE AND MALICIOUS CODE SECURITY POLICY

The intent of this policy is to better protect assets against attack from malicious programmes.

- Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any company resource.
- No unauthorised software will be downloaded and installed on end user machines without express approval from the IT team.
- System users will not execute programmes of unknown origin, as they may contain malicious logic.
- Only licensed and approved software will be used on any company computing resource.
- All licensed software will be write-protected and stored by the IT team.
- users will scan all files introduced into its environment for virus, hostile and malicious code before use.
- The IT team will ensure that obtains and deploys the latest in virus protection and detection tools.
- All information systems media, including disks, CDs and Universal Serial Bus (USB) drives, introduced to the environment will be scanned for virus, hostile and malicious code.
- All emails will be scanned for virus, hostile and malicious code.
- All internet file transfers will be scanned for virus, hostile and malicious code.
- The unauthorised development, transfer or execution for virus, hostile and malicious code is strictly prohibited.
- All users will report any suspicious occurrences to his/her supervisor or the IT team immediately.
- All company systems will be protected by a standard virus protection system.
- Virus engines and data files will be updated on at least a monthly basis.
- Viruses that are detected on a user's workstation will be reported to the IT team immediately for action and resolution.
- Anomalous behaviours of any software programme will be reported to the IT team immediately.

POLICY

Bring Your Own Device (BYOD) and Acceptable Use

Location: [INSERT LOCATION]

Effective Date: [INSERT DATE]

Revision Number: [INSERT #]

About This Policy

Information security policies are the principles that direct managerial decision making and facilitate secure business operations. A concise set of security policies enables the IT team to manage the security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorised behaviour for personnel approved to use information assets, such as laptops, tablets and smartphones.

Applicability

The BYOD and Acceptable Use Policy applies to all employees, interns, contractors, suppliers and anyone using assets. Policies are the organisational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by or its designated representatives.

BYOD POLICY

This policy provides guidelines for using personally owned devices and related software for corporate use.

Applicability

The BYOD policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by appropriate management or a designated representative.

Furthermore, based on the amount of personally identifiable information employees work with, management reserves the right to determine which employees can use personally owned devices and which cannot.

General Policy

recognises that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by for corporate use:

- Desktop computers
- Laptop computers
- Tablets
- Personal digital assistants (PDAs)
- Smart phones
- Portable music players

Reimbursement

may provide reimbursement for the purchase of personally owned devices up to £_____ to eligible employees. However, is not responsible for any additional costs associated with learning, administering or installing these devices.

Registering Devices

All personally owned devices must be registered with ’s IT department.

End-User Support

As a general rule, users of personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

IT will support personally owned devices as follows:

- The user will be required to allow IT to load security software on each device.
- The user will be required to allow IT to install remote wiping software on each device.
- Upon request, the IT team will install the necessary synchronisation software to the user's desktop or notebook computer.

Device Security

The user should follow good security practices including:

- Password protect all personally owned devices
- Do not leave personally owned devices unattended

Release of Liability and Disclaimer to Users

hereby acknowledges that the use of personally owned devices in connection with business carries specific risks for which you, as the end user, assume full liability.

In the case of litigation, may take and confiscate a user's personally owned device at any time.

ACCEPTABLE USE POLICY

This policy provides rules for the acceptable use of personally owned devices on the corporate network.

Applicability

The Acceptable Use Policy applies to all employees, contractors, suppliers and any other person using or accessing information or information systems. Exceptions to this policy must be approved by the CIO or a designated representative.

General Policy

Users that wish to access the network using their personally owned computer may do so using only -authorised software and only with the approval of the user's supervisor and the IT department.

Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the network, the user will NOT:

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send junk email or spam to anyone
- Attempt to send a massive amount of email to a specific person or system in order to flood their servers

Authorisation of Devices

IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

IT will install a digital certificate on each personally owned device, which will authenticate the user.

Third-Party Applications on Devices

IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

As the number of approved applications continually evolves, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading it on the device.

Remote Wiping

While does not own the device, they do own all company data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time. Not only will company data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk.

Furthermore, the user must agree to a full wipe of the personally owned device if they leave . This may result in the loss of both company and personal data on the device.