CYBER PATH
POLICE & ACADEMIA
TALENT HORIZONS

THE
CYBER
RESILIENCE
CENTRE
NETWORK

Cyber Business Continuity and Security Policy Review

This report contains the results of two services, which we combined into a single report for the client's ease

Services Provided:	Cyber Business Continuity Review Security Policy Review
Created for:	Engineering Ltd
Report Submitted:	03/01/2026
Student Assessor:	Alex Thomas

Contents

Your Assessment

Thank you for entrusting our team at Cyber PATH to help you. Our unique partnership between Policing, Business and Academia strives to support organisations like yours on their journey to Cyber Resilience. We recognise that this may be the first time you have considered contracting a cyber service and you might be unsure what to expect or how to act on these findings. Our team are dedicated to making the process as simple and transparent as possible, to help you understand the risks highlighted in this report and how to improve on them. Please raise any questions at all with us. We are here to help you learn as much as possible – there are no silly questions here!

Assessment Information	
Services completed	Cyber Business Continuity Review Security Policy Review
Assessment Completed By	Cyber PATH Team
Date Completed	14/12/2025
Overseen By	Cyber PATH Student Supervisors

Executive Summary

Cyber PATH have been provided the opportunity to review the Business Continuity Policy and Information Security policy [redacted]. From the conversations with the members of the [redacted] team – alongside the provided documentation, it is clear that a considerable amount of effort has been made to create practical and informed policy that meets the needs of the organisation.

This has been demonstrated throughout the engagement, with attention to detail on the elements of the Business Continuity management system and Information Security policies in place. There has also been a demonstrably clear focus on providing actionable guidance for employees at all levels that aims to enhance the security culture of the organisation.

Having been invited to make contributions to the ongoing organisation-wide conversation, it has been possible to make granular and mainly organisational observations relating to points for further development in the policy documents that have been provided to the assessment team. This feedback should not detract from the totality of the work that has been done but aims to contribute to the holistic considerations for ongoing development and improvement that are essential for the living and breathing documents that organisations of your maturity require.

This report should not be taken in isolation, and you are invited to get in touch for further discussion around any of the points raised at your convenience.

Documents Reviewed

The process of conducting a Cyber Business Continuity Review, or a Security Policy Review involves round table discussion with all relevant stake holders. Organisational continuity arrangements may be in a single document, or dispersed among different areas, documents, processes, and people. Here it is specified what documents were made available to the assessment team in addition to the conversations that have been had between the assessment team and [redacted].This aims to contribute to the focus on considerations further to the service delivered.

Table 1 - Documents received and evaluated for the Cyber Business Continuity Review and Security Policy Review.

Document Received	Relevant Service
Information Security Policy (for issue) V1.0 FINAL	Security Policy Review
Data Breach and Incident Response Policy (for issue) V1.0 FINAL	Security Policy Review
[redacted] Business Continuity Policy (Final)	Cyber Business Continuity Review

Cyber Business Continuity Review

Table 2 provides points for consideration derived from the international standard for Business Continuity Management Systems (BCMS), ISO/IEC 22301:2019, and is structured to introduce topics for review and conversation based on comments and observations. For each question, the relevant material from the documents reviewed (Table 1) are referenced appropriately, and actions are suggested as considerations for the [redacted] team moving forward.

Table 2 - Cyber Business Continuity Review table.

CBC review	Comments observations	Reference	Action
Has the client identified aims and objectives for cyber business continuity?	The policy sets out its posture on business continuity aims and objectives across the introduction and summary, alongside a business continuity statement. These sections set out the importance of developing and maintaining effective BCP measures but do not share explicit aims and objectives. Multiple statements are made in the BCP Summary section that could be interpreted as aims and objectives, but these reference the business continuity plan as a whole.	*BUSINESS CONTINUITY STATEMENT,* *BUSINESS CONTINUITY INTRODUCTION, BCP Summary.*	Consider the value of a definitive set of aims and objectives for the business continuity policy, and assess whether this addition would provide a platform for continuous improvement.
Is there an existing BC Policy?	[redacted] has shared a draft business continuity policy, that was last updated in August of 2022.	*BC Policy v2.1 Jan 2012*	None
Is there an existing BC Plan and if so, has this ever been exercised?	An existing BC plan has been constructed, with no clear statement on the aim of regular exercising of the plan beyond the Business Continuity Statement that shares that the policy is regularly reviewed as part of ESG – which is here taken to mean 'Environmental, Social and Governance', and the Risk Committee. The planning scope and documentation also identifies that Recovery Capabilities that fall within the BCP are validated via internal testing. It cannot be inferred from the policy body whether scheduled exercising of the BCP contributes to the ongoing validation of the business continuity plan, and it was confirmed in conversation that there hasn't been scheduled exercising of the plan.	*BUSINESS CONTINUITY STATEMENT,* *PLANNING SCOPE AND DOCUMENTATION*	Consider the value of making the output of the regular review process of the [redacted] Business Continuity Plan available where possible and referencing it directly in this policy. Consider the value of ongoing validation of your BCP utilising regular exercising of the plan, and if it is determined to add value to your body of policy then consider sharing the frequency and expectations around exercising plans in your body of policy.
Is there an existing Disaster recovery Policy	A disaster recovery policy has not been made available to the assessment team and is not		Consider the value of creating a Disaster Recovery policy that may promote development in responding

	referenced in the Business Continuity Policy. The Major Incident and Crisis plan for on-site [redacted] was discussed as covering some of the high-level points that a disaster recovery policy may cover.		to the five impact types that the scope of this policy concerns itself with.
Does BC policy reference What systems, processes and information are in scope?	The BC Policy identifies the concerns of the Business Continuity Plan in its BCP summary. This section focuses on identifying what the BCP incorporates into itself in order to meet five goals. This identifies procedures and strategies that may utilise or refer to information or systems, but these are not referenced directly or via a statement on business impact analysis. An exclusion is shared in the BUSINESS CONTINUITY STATEMENT for on-site customer events – which is covered by the aforementioned Major Incident and Crisis plan.	*BCP Summary, PLANNING SCOPE AND DOCUMENTATION*	Consider the value in more clearly defining what products and services are within the scope of your business continuity programme. Where existing inclusions or exclusions are made, consider if you would benefit from a focused definition of the scope of the Business Continuity Plan and the Business Continuity Policy – defining inclusions and exclusions.
Has the client impact assessed the elements in the scope of the BC policy	Clear references are made to the regular annual review of the BCP programme in the BUSINESS CONTINUITY STATEMENT, which is owned by the [redacted] Risk Committee. There is not a clear reference to the development and maintenance of a business impact analysis for the organisation.	*BUSINESS CONTINUITY STATEMENT*	Further to our conversation, consider the value of conducting a business impact analysis. If a business impact analysis has been completed and is maintained, then consider the value of sharing this as a part of the roles and responsibilities that have arisen as a part of the BCP programme.
Has the client identified maximum tolerable downtime for the services/products in scope? Has the client identified recovery point and recovery time objectives and documented these in the BC policy?	The Appendix of the plan clearly shares the RPO and RTO of server files but does not attach these to business continuity targets and solutions.	*Appendix A*	Consider the value of establishing internal objectives for RPO, RTO, and MTD and comparing these to the provided third-party services that are mentioned in the annex.
Does the BC policy reference organisational roles and responsibilities for BC	The policy is clear in the support that the BCP has, alongside providing ownership of the [redacted] BCP programme. The decomposition of the Crisis Management Team into the expected participants in each group ensures a thorough reference to who is likely to have roles and responsibilities in relation to BC.	*GOVERNANCE,* *CRISIS MANAGEMENT*	Consider whether the body of policy would benefit from the listing of roles within groups that own substantial responsibility for documents, processes, and their respective maintenance and improvement. In instances where roles and responsibilities can be expected to change semi-frequently, consider the value of creating a live document to

	Beyond the CMT and the total ownership of the ongoing BCP programme by the [redacted] Risk Committee, there are no specified roles and responsibilities.		share these roles and then pointing to it in the body of policy.
Has the client identified legal and regulatory compliance	The BUSINESS CONTINUITY INTRODUCTION identifies an express aim of the BCP to minimise the regulatory impact of major internal or external incidents, but there is no specified objective to identify and maintain compliance with regulatory or legal objectives.	*BUSINESS CONTINUITY INTRODUCTION*	Consider documenting legal and regulatory requirements in a separate policy such as a legal and regulatory register. Assess the value of referencing this legal and regulatory register in the Business Continuity Elements and Review Arrangements section of the policy.

Security Policy Review

Table 3 provides points for consideration derived from the international standard for an Information Security Management System (ISMS), ISO/IEC 27001:2022, and is structured to introduce topics for review and conversation based on comments and observations. For each question, the relevant material from the documents reviewed (Table 1) are referenced appropriately, and actions are suggested as considerations for [redacted] moving forward.

Table 3 - Security Policy Review table.

IS policy review	Comments observations	Reference	Action
IS Policy Overview	The policy overview is as follows: • Introduction • Internet Access • Computers and Internet Usage – Inappropriate Use • Computer and Internet Usage – Security • Monitoring and Incident Handling • Use of Personal Equipment for Company Business • Computers and Internet Usage – Penalties • Information Security Awareness Training • Data or Security Breaches	*Information Security Policy (for issue) V1.0 FINAL.pdf*	Consider the value of developing the information security policy to meet with an external standard that will help provide focus in key areas such as the development of roles and responsibilities, scope and applicability, and terms for review and continual improvement.
IS Purpose and Objectives	Purposes and objectives of the policy are outlined in the introduction of the policy, and these show clear focus on ensuring the CIA triad is not disrupted, ensuring compliance with relevant legislation, understanding responsibility, enhancing security awareness, and protecting information and assets.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Introduction*	Consider the value of identifying and defining the aims and objectives of the policy in a section named to reflect this.
IS policy scope and applicability- (does it include the whole organisation, sub-departments, exclusions, services, processes).	The Introduction section of the policy states that the policy 'includes, but is not limited to' desktops, laptops, printers, and mobile device, and applies to the internet, company email and other messaging services, and any other hosted IT services. No exclusions are identified.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Introduction*	Consider the value of identifying and defining inclusions and exclusions for the scope and applicability in a section named to reflect this. The level of specificity may promote discussion and clarity that could be further explored at your discretion if a section was given for policy scope and applicability.
Does it reference the risk assessment/management framework	The Information security policy and Data Breach and Incident Response Policy does not identify a risk assessment or management framework.	*Information Security Policy (for issue) V1.0 FINAL.pdf* *Data Breach and Incident Response*	Consider the value of utilising an existing risk assessment or risk management framework to help focus continuous improvement of the body of policy.

		Policy (for issue) V1.0 FINAL.pdf	
Does it reference organisational roles and responsibilities for IS	Responsibilities are set clearly in the introduction as to the need for awareness of the need for information security, alongside ensuring that everyone understands their own responsibilities. Clear responsibilities are set for everyone to be aware of their obligations and compliance with relevant legislation. Responsibilities are further identified in each section of the Information Security policy, relevant to the section being discussed. These are folded in with best practice recommendations and guidance. Additional roles beyond the operational responsibilities of all employees are not discussed in the Information Security Policy. Additional roles, risk ownership, and responsibilities are identified in the Data Breach and Incident Response policy – including additional expectations and responsibilities for the Information Security Manager. Further to this, roles and responsibilities are identified for the owners of monitoring and alert services, as well as blanket applications of responsibility to all employees, contractors, or third parties.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Introduction* - *Internet Access* - *Computers and Internet Usage – Inappropriate Use* - *Monitoring and Incident Handling* - *Use of Personal Equipment for Company Business* - *Computers and Internet Usage – Penalties* - *Information Security Awareness Training* - *Data or Security Breaches* *Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf* - *Responsibilities*	Consider further discussion of the precise roles and subsequent responsibilities that have arisen in response to information security objectives. This granularity can promote discussion and clarity, while more generic coverage can allow for certain topics or areas to remain unexamined. Consider organisation of these roles and responsibilities in a section that is separate to the ongoing operational expectations of all employees.
Does it reference organisational controls and control objectives, either directly (e.g., in a statement of applicability) or indirectly, such as: • **Mobile devices and teleworking** • **Human resources security** • **Asset management** • **Information classification** • **Access control** • **Cryptography** • **Physical and environmental security** • **Operations security**	Organisational controls are clearly identified both in the Information Security policy and in the supporting Data Breach and Incident Policy. These focus on distinct areas of information security and lay out organisational controls and expectations for employees. No direct statement of applicability is made regarding organisational controls in the Information Security Policy. No direct statement of applicability is made regarding organisational controls in the Data Breach policy, but there is a clear commitment made to continuous improvement in the follow up to disruptive incidents, and it's clearly stated that the body of policy has ongoing oversight from the Board through the lens of incidents and subsequent additional controls.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Introduction* - *Internet Access* - *Computers and Internet Usage – Inappropriate Use* - *Monitoring and Incident Handling* - *Use of Personal Equipment for Company Business* - *Computers and Internet Usage – Penalties* - *Information Security*	Consider the value of a direct statement of controls and control objectives in the form of a statement of applicability, sharing the support and ongoing validation from the organisation, alongside how this is achieved. Assess whether the organisation would create additional utility in the body of policy from exploring the controls and objectives that are shared in the attached examples.

• **Communications security** • **Systems acquisition, development, and maintenance** • **Supplier relationships** • **IS incident management**. • **IS aspects of business continuity** • **Compliance**		*Awareness Training* - *Data or Security Breaches* *Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf* - *Responsibilities* - *Procedure*	
Does it reference IS policy review responsibilities, periods?	Review responsibilities are set out in the Data Breach and Incident Response policy as to the reporting of incidents each quarter, alongside recommendations for additional controls. This does not necessarily suggest that this policy is subject to scheduled reviews. The Information Security Policy does not share a schedule for the regular review of responsibilities.	*Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf* - *Procedure* *Information Security Policy (for issue) V1.0 FINAL.pdf*	Consider the value of sharing the scheduled regular review periods for the policy documents, alongside ownership of this responsibility.
Does it reference what happens if this policy is breached	The Information Security Policy identifies penalties for Computer and Internet misuse and identifies that misuse of company technology may be treated as a disciplinary matter – the consequences of which are clearly stated to reach dismissal where appropriate. The policy clearly states that information systems and company assets may be monitored to ensure accordance with the policy.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Computers and internet Usage – Penalties* - *Monitoring and Incident Handling*	Determine if additional utility would be derived from the body of policy if the disciplinary options made available to the organisation were scoped to apply to all policy non-conformity, instead of the misuse of company technology and facilities, emails, the message service, or the internet. This could be used to facilitate the direction of other policy areas to this section more effectively.
Does it reference how monitoring adherence to the ISP is achieved	It is made clear that company assets are subject to monitoring to ensure adherence with the body of policy.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Monitoring and Incident Handling*	None
Does it reference how security of information is to be maintained	Guidance is given to employees in relevant sections as to means by which security of information is to be maintained. This guidance is distributed across different sections and is discussed through recommendations of operational practice such as encrypting sensitive information before sending it, avoiding circumventing security measures, or running virus protection software on personal machines that contain company information.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Computers and internet Usage – Security* - *Computers and internet Usage – Inappropriate Use* - *Use of Personal Equipment for Company Business*	Consider the value of centralising the controls and guidance that have been determined as relevant for the purposes of keeping the information system secure and assuring the security of information.
Does it reference the use of WiFi networks	There is no mention of WiFi networks beyond the requirement to disconnect from WiFi in the case that an employee suspects they have engaged a phishing email.	*Information Security Policy (for issue) V1.0 FINAL.pdf*	Consider whether it would enhance the posture of your policy to share the expectations relating to the use of company WiFi.

		- *Data or Security Breaches* *Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf* - *Example breach and what to do*	
Does it reference malware protection	The information security policy clearly states that it is a violation of policy for an employee to disable the provided virus scanning software on devices provided by the company, as well as stating that the condition of allowing corporate data onto personal machines is partially fulfilled with the use of virus protection software.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Computer and Internet Usage – Security* - *Use of Personal Equipment for Company Business*	Consider whether it would enhance the posture of your policy to centralise expectations and responsibilities arising from malware and virus protection.
Does it reference Software Security	There is no defined section on software security, but a clear reference to the requirement for the use of remote support software and managed software updates, alongside virus scanning software.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Computer and Internet Usage – Security* - *Use of Personal Equipment for Company Business*	Consider whether it would enhance the posture of your policy to share the expectations relating to the use of software in the context of keeping software secure.
Does it reference Intellectual property	Intellectual property is not mentioned in the assessed policies.	*Information Security Policy (for issue) V1.0 FINAL.pdf* *Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf*	Consider the possible value of sharing the relevant compliance and conformity with considerations relating to Intellectual Property.
Does it reference equipment and hardware	Whilst it is made clear that systems and hardware that are company owned or purchased remain in the scope of this policy, there are no responsibilities for end users shared that relate to the condition or integrity of hardware.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Monitoring and Incident Handling*	Consider whether it would enhance the posture of your policy to centralise expectations and responsibilities arising from equipment and hardware.
Does it reference access to systems	Guidance is made clear throughout the Computer and Internet Usage section that passwords should not be revealed to others or stored in a way that could be foreseen as to be predictable or easy to compromise. The need for devices to remain password protected is not explicitly stated either for company owned devices or personal devices. The password guidance does not suggest any complexity requirements.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Computer and Internet Usage – Security* - *Use of Personal Equipment for Company Business*	Consider setting expectations that all machines must be password protected. Where the requirements of an employee to store information on their own device are shared, consider the value of creating an expectation that the device is password protected, as well as providing employees with password creation guidelines that set expectations for complexity.

Does it reference data security and email	Email use is clearly specified in an applicability statement in the introduction of the policy but does not mention any technical security controls relating to how email is used. There is clear guidance throughout the policy as to the guidance employees should follow to contribute to good email and data security, and what behaviour is expected from them regarding email access and data security.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Introduction* - *Internet Access* - *Computer and Internet Usage – Inappropriate Use*	Consider whether it would enhance the posture of your policy to centralise expectations and responsibilities arising from data security and email etiquette.
Does it reference data security and cardholder data	No reference is made to cardholder data or data security in the context of digital payments or transactions.	*Information Security Policy (for issue) V1.0 FINAL.pdf* *Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf*	Consider whether it is relevant to share your controls and compliance relating to data security in the context of cardholder data or payment infrastructure, for example with respect to PCI-DSS
Does it reference data security and the internet	Internet and internet access are clearly stated as a provision to allow employees to perform the requirements of their role, and responsibilities are set out as to the reasonable use of internet being to support specific work-related duties. Technical controls are identified as essential to the provision of internet for employees, with an explicit statement that no efforts should be taken to circumvent of subvert any security measures that affect company devices or any internet accessible system. Employees are also invited to reach out to check what constitutes acceptable use with an appropriate manager.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Internet Access* - *Computers and Internet Usage – Inappropriate Use*	Consider the value of expanding the scope of the internet usage section to explain more specifically where this constitutes acceptable use, and examples of what may constitute unacceptable use – This granularity can promote discussion and clarity, while a more generic scope of applicability can allow for certain topics or areas to remain unexamined.
Does it reference data security and mobile or portable devices	Mobile devices such as tablets and phones are captured in the introduction as included in the scope of the policy. Personal and company owned mobile devices are permitted for company business.	*Information Security Policy (for issue) V1.0 FINAL.pdf* - *Introduction*	Consider whether it would enhance the posture of your policy to centralise expectations and responsibilities arising from mobile devices both in a company owned and personally owned capacity.
Does it reference IS incident management	The Data Breach and Incident Response Policy clearly identifies the ownership of responsibility for incident response and management, as well as providing a procedure to employees to follow to ensure timely reporting of incidents. Further to this, the policy provides an example incident to further enhance employee awareness. Continuous improvement is suggested when discussing how the incident will be closed out, involving the 'planning and implementing' of 'preventative action to avoid any further recurrence'. Conversations made clear that there has not yet been the time to schedule regular risk assessments for the validation and continuous improvement of the system.	*Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf* - *Responsibilities* - *Procedure*	Consider the possible value of further sharing how incident management ties in with ongoing risk assessments in providing an avenue for continuous improvement.
Does it reference legal and regulatory compliance	The body of policy references the intention to remain compliant with the General Data Protection Regulation (GDPR). The Information	*Information Security Policy (for issue) V1.0 FINAL.pdf*	Consider documenting legal and regulatory requirements in a separate policy such as a legal and regulatory register. Assess the value of referencing

	Security Policy does not mention the Data Protection Act 2018 (DPA). The Data Breach and Incident Response Policy mentions both DPA and GDPR.	- *Introduction* - *Monitoring and Incident Handling* *Data Breach and Incident Response Policy (for issue) V1.0 FINAL.pdf* - *Responsibilities*	this legal and regulatory register in the Information Security Policy

About the Cyber Resilience Centre Network

The National Cyber Resilience Centre Group and Cyber Resilience Centres are funded and supported by the Home Office and policing in a not-for-profit partnership with the private sector and academia to strengthen our national cyber resilience across SMEs and the supply chain.

At a national level, NCRCG is building a coalition of police, government, large employers and organisations, and academia to ensure a collaborative and coherent approach to cyber resilience.

NCRCG and its National Ambassadors and the CRC network are committed to investing in the next generation of cyber experts. As such, NCRCG has launched Cyber PATH in partnership with the CRC network and over 45 universities.

The nine CRCs operate across England and Wales. They serve SMEs in their locality helping to build cyber resilience against threats that are specific to them. Cyber PATH empowers students to work with their regional CRC in meeting the requests brought to them by local businesses.

Each CRC retains the freedoms to deliver tailored, trusted and fully funded support, with NCRCG providing insight and solutions at a macro level.

You can learn more about the work of the NCRCG here. We can help your own customers and suppliers too, so spread the word.

There's more to the Cyber Resilience Centres...

There are many additional ways to engage with your Regional CRC. If you haven't already, you can join the community, which is free of charge. This membership includes practical, government-approved guidance, as well as regular information updates to keep you informed of our other help and services on offer, including:

- **Educational Events** - CRCs run regular webinars and events on a range of topics relevant to your small business or third sector organisation

- **Funded solutions** – CRCs offer a range of services like this one, which are designed to address the most pertinent risks affecting SMEs, as identified by policing and Government.

- **Cyber Essentials Certification** - If you are planning to achieve Cyber Essentials or Cyber Essentials Plus certification, your Regional CRC can refer you to IASME who have a list of local suppliers in your region that provide this.

Find your Regional Cyber Resilience Centre here.

Get in touch with us at engagement@cyberpath.co.uk if there's anything else we can help you with.