Appendix A: Cyber Security Strategy

Birmingham City Council Cyber Security Strategy

2020-2024

What is Cyber Security?

Cyber security is the practice of ensuring the confidentiality, integrity and availability of information using the technologies, processes, and people behaviour practices designed to protect the IT infrastructure, applications and data from attack, damage, or unauthorised access that we use in our everyday lives.

Cyber Security Strategy alignment to Council Delivery Plan and ICT and Digital Strategy ("ICT&D Strategy")

The Council is determined to make Birmingham a fair and thriving city where all citizens have the opportunity to achieve their potential and share in the city's success. The Council is pursuing this ambition against an increasingly complex public service landscape as we face significant social, fiscal, and political challenges. This includes increasing demand for vital services; changes to citizens' needs and expectations; diminishing resources; the ongoing climate emergency; an uncertain national political picture, complicated by Brexit; and the unprecedented Coronavirus pandemic.

In November 2020 the Council approved its Delivery Plan which describes two types of activity which will be delivered in parallel through to May 2022, ensuring we deliver our short and medium-term commitments alongside shaping our approach for realising our longer-term goals.

First, it sets out the work that will be undertaken over the next 18 months so that the Council, working in partnership with others, can maximise the opportunities it has to tackle inequality and address both long-standing and novel challenges facing the city, including, for example, climate change. In the first instance this will be about understanding the challenges and opportunities in more detail and then developing comprehensive proposals for change that include business case, organisational change proposals and then a timeline for delivery. Working in this way we aim to improve outcomes and balance the books up to and beyond 2022. This is about understanding where the City can and should be over the next 10 to 20 years and making sure we put in place now the necessary strategies and capacity to enable it to happen.

Secondly, it sets out specific deliverables and commitments we will achieve over the next 18 months and how we will do this, aligned to our finances and accompanied by our refreshed Performance Management Framework. This activity focuses on "getting the basics right" as well as delivering on other critical priorities, including ensuring the city is ready for and benefits from the Birmingham 2022 Commonwealth Games and supporting the city to respond and then recover from the Coronavirus pandemic. This activity includes tasks that are specific to particular areas of the Council as well as cross-cutting priorities involving several Council services which need to be delivered in a joined-up way, both across the organisation and partnerships.

The activity in the Delivery Plan is driven by and contributes to our existing six outcomes for Birmingham to be:

- An entrepreneurial city to learn, work and invest in
- An aspirational city to grow up in
- A fulfilling city to age well in
- A great city to live in
- A city whose residents gain the most from hosting the 2022 Commonwealth Games
- A city that takes a leading role in tackling climate change

In October 2016 Cabinet approved the Council's ICT&D Strategy, which formed a new framework for ICT service operation around 6 key themes:

1. Integrated ICT and Digital Services - to deliver a reliable, flexible, integrated, secure, accessible and well managed service.
2. Digital facilitation - to enable our stakeholders to participate and fully contribute to the growth of the Digital Economy and Digital Society and create a Digital Culture.
3. Insight - to become more data centric – so we can create the capability to turn information into insight.
4. Commissioning - to deliver 'Value for Money' services through the commissioning of excellent ICTD.
5. Governance - to deliver the effective management of ICTD.
6. Innovation - to be innovative; to make changes to what's established, by introducing new methods, ideas, and solutions.

The ICT & Digital strategy's overarching principles to "Simplify, Standardise and Share" ensures that the council maximises the benefits from investment in new technology and digital services by:

- Simplify – the way we operate, in order to add value and drive up efficiency.
- Standardise – the way we operate, emulating the best and enabling agility.
- Share – collaborate, innovate and inform

These design principles will ensure that we:

- Consolidate services and applications
- Re use and rationalise.
- Share with and learn from partners, internally and externally,
- Don't reinvent - learn from others and share.

The ICT & Digital strategy is a key enabler in the Council achieving its priorities and outcomes as described in the Council Plan and updated Delivery Plan. One of the key areas of focus for the ICT & Digital strategy is "improving information assurance, maturity, risk management and safety of personal data". The Council will never achieve the outcomes for the Citizens of Birmingham if we cannot adequately protect the data used in the delivery of vital public services.

This Cyber Security Strategy and roadmap supports that key area of focus and includes protecting an ever-increasing agile workforce, growth in the uptake of technologies such as cloud-based systems, internet-enabled services, mobile devices, high-speed broadband and together with the digital agenda on utilising/sharing more data of all forms to develop public services means that cyber security will be increasingly tested, and implementation of the Cyber security strategy will require investment in extra resource and technologies.

The Cyber Security strategy is designed to drive the Council's security posture forward. The Council has already built a baseline to ensure that it has a robust and systematic security posture that protects against most types of threats. The Baseline follows industry best practices such as the National Cyber Security Centre (NSCS), National Institute of Standards and Technology (NIST) and ISO27001. NSCS guidance of 10 steps to cyber security and the NIST security objectives will be followed in conjunction with creating a risk-based information security management system (ISMS). An ISMS will enable the Council to achieve ISO 27001 accreditation. This is an externally audited certification to demonstrate that the Council has a core security system in place with a baseline security posture that gives the Council fundamental security processes and protection.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

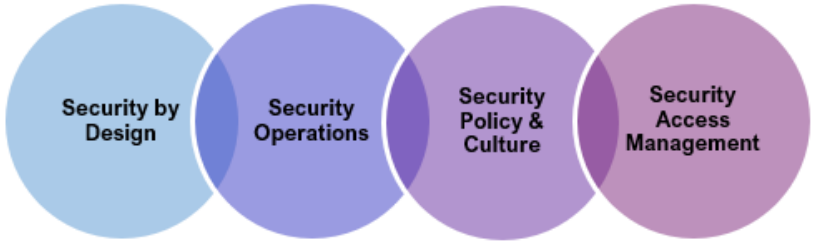
For more information go to **www.ncsc.gov.uk** **@ncsc**

Birmingham City Council Cyber Security Strategy

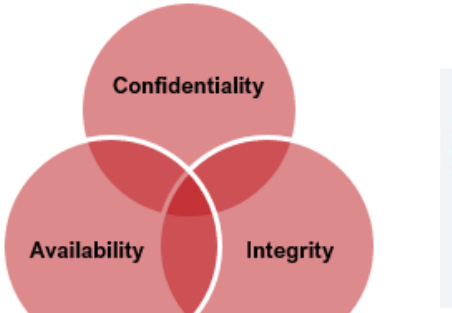
Our vision is to be a trusted cyber security champion in the UK public local authority sector

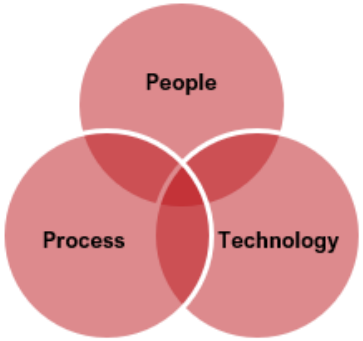
Our mission is to protect BCCs critical infrastructure, applications, assets and customer data while enabling BCC to deliver trusted secure services

Strategic Themes



Security Objectives

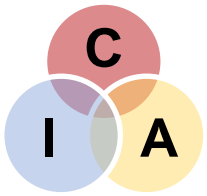




Our Approach

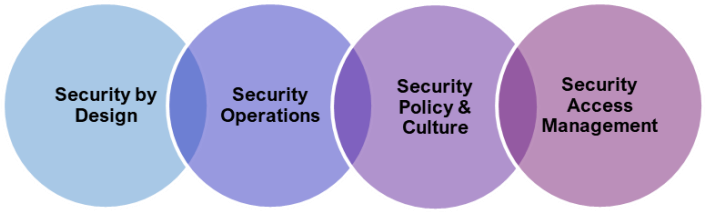
To achieve our vision of becoming a cyber security champion, the strategy approach created will organise and improve the overall security posture of our services driven by adopting the information security principles, organised into 4 main strategic themes and underpinned by National Institute of Standards and Technology (NIST) objectives**.** We are adopting this non-proprietary, common NIST cyber security framework compatible with technical and industry standards including ISO27001, covering the key interrelated components of **people, process and technology**. The strategy will be continuously under review, iterate and improved.

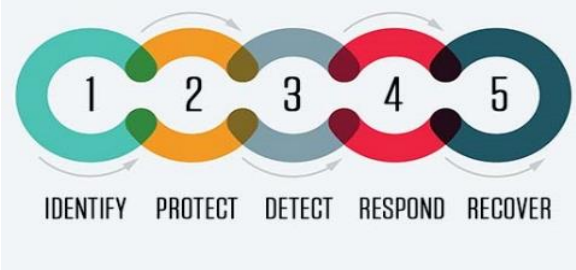
The delivery of the Cyber Security strategy and function will harness best practice CIA principles of information security



- **Confidentiality** - ensure that the necessary level of controls is enforced at each junction of data processing and prevent unauthorised disclosure.
- **Integrity** - assurance of the accuracy and reliability of information and systems is provided and any unauthorised modification is prevented
- **Availability** - ensure reliability and timely access to data and resources to authorised individual

The Cyber Security strategy is centred around four strategic themes:





The strategy is to be underpinned by the NIST Cyber Security Framework objectives:

This approach will enable the continuous improvement of the security maturity of the organisation, as well as maintaining and updating ongoing BAU activities and project strategic support (security advice, security incident management, project assurance, monitoring activities, vulnerability scanning, penetration testing) to ensure they remain fit for purpose.

The Four Strategic Key Themes:

Theme Name	Key Goals	Security Objectives
Theme 1 –Secure by Design	Ensure security by design is in place for or all IT systems including future innovations. All security activities are planned as part of programmes/projects delivering secure trusted solutions to our customers Ensure existing and new Cyber Security tools are leveraged, selected and optimised to protect BCC and its customer.	**Identify** **Protect** **Detect**
Theme 2 – Security Operations	Ensure we have security capabilities in place to defend BCC, our customers, and our employees from cybercrime attacks that lead to malicious activity, data breaches, destruction of key digital information. Ensure we have tested and proven capabilities to monitor and recover from security-based threats.	**Protect** **Detect** **Respond** **Recover**
Theme 3 – Security Policy & Culture	Ensure we have security policies that are aligned to industry best practice to fit BCC and are kept up to date, accessible, communicated and embedded in BCC Ensure that we have a strategic and successful approach for security user education and awareness at all levels at BCC including our customers and partners. Achieve a risk based ISO27001 information security management system	**Identify** **Protect**
Theme 4 – Security Access Management	Establish and enable centralised secure access and regulation for BCC and its partners **providing** the right levels of access to the required enterprise resources for delivering trusted secure services to customers. Ensure that BCC and its trusted partners adhere to identity and access management controls including but not limited to people, processes and systems that are used to manage access to enterprise resources	**Protect** **Detect**

The security activities for each of the themes will follow three Cyber Security Maturity levels detailed below to ensure basic and foundational building blocks are in place to improve and strengthen the security posture.

Maturity level	Description
Foundation	Foundation activities need to be completed to ensure a managed security function can be developed. This includes having full visibility of BCC cyber landscape and current security tools, policies in place, obtaining Cyber Essential certification and ISO27001 gap analysis completed
Managed	Security function is being managed across all areas of people, process and technology areas. ISO27001 preparation work identified and is in progress.
Optimised	A robust security function is in place and fully optimised across all people, processes and technology areas. ISO27001 Certification has been achieved.

This strategy will improve our current security around end-user computing, servers, network, and the gateway security products to ensure that we have the correct security services that enable our wider transformation around Hybrid Cloud, Digitalisation, and Agility, by:

- Ensuring that Cyber Security becomes an ***enabler*** to deliver secure current and new services to the Council's Transformation programmes.
- Ensures that the Council have an overall service that provides the 'class-leading' cyber security protection which our city and citizens deserve and demand.
- Ensure effective and enduring protection of cyber security, privacy, and resilience for the Council, its citizens and the digital assets we control.
- Support the Digital Transformation Agenda by ensuring that the council's digital services are secure and private while still being easy-to-use.
- Develop and implement effective security standards to prevent unacceptable loss of sensitive data or assets and foster the overall group coordination and alignment on cyber strategy and controls.

Cyber Security RoadMap

In line with the new Cyber Security Strategy, we are building secure, sustainable, and innovating capabilities and processes. We aim to become an example to follow amongst the public sector and go-to council for colleagues while influencing and improving the BCC brand in public services.