NORHAM PARISH COUNCIL

Website: https://norhamlife.co.uk

Cybersecurity checklist

A. Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

B. Many of the steps that councils can take to limit the risk and impact of a personal data breach are relatively simple to implement but require effective policies and controls to implement. Good information security crosses over a number of policies – it is not just a matter of putting in place an information security policy. The checklist below sets out the key issues that a council should deal with, and which should be implemented where appropriate across the entire suite of internal policies.

Glossary

a) "*Acceptable use policy*" or fair use policy is a set of rules applied by the owner, creator or administrator of a network, website, or service, which restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

b) *"Bring Your Own Device" ("BYOD")* policy is useful where staff are permitted to use their own tablets, mobile devices and other IT equipment and deals with appropriate security measures that they should comply with.

c) "*Cyber security"* is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

d) *"Firewall"* is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

e) *"Multifactor authentication*" is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction for example using a password and a separate delivered pin number (sometimes described as "2 step" authentication).

f) *"Network security policy"* is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the security/ network security environment.

g) *"Penetration testing" (*also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

h) *"Red teaming"* using consults to test your physical and systems security.

i) *"Remote access policy"* is a document which outlines and defines acceptable methods of remotely connecting to the internal network.

j) *"Remote access"* is the ability to get access to a computer or a network from a remote distance.

k) *"Wifi"* a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

Do you have appropriate policies in place?

a) Information security policy
b) Privacy policy
c) "Bring Your Own Device" ("BYOD") policy
d) Remote access policy
e) Network security policy
f) Acceptable use/internet access policy
g) Email and communication policy

Depending on how your policies are structured, the issues below may appear in one or more of these policies.

a) Are your policies checked and updated on a regular basis and enforced?
b) Is there a council member with responsibility for cyber security?
c) Do you have clear responsibility for cyber security, with clear reporting lines and
d) decision-making authority?
e) Do you ensure physical security of premises?
f) Do you allocate sufficient budget to cyber security?
g) Do you subscribe to cyber security updates so that you are aware of threats?
h) Do you have an effective breach response plan, and do you test and update it regularly?
i) Do you have cyber breach insurance in place?

People

a) Do you have appropriate mechanisms for staff and councillors to be able to report suspicious emails quickly and effectively?
b) Do you train staff and councillors on cyber security regularly?
c) Do you test staff and councillors, for example by sending spoof phishing emails?
d) Do councillors and staff undertake reviews to ensure that they understand cyber security risks, and are results checked to ensure improvement?
e) Do you have proper processes for when staff or councillors join or leave the council, and are they applied in practice?
f) Do staff and councillors understand the risks of using public wifi? Do you conduct appropriate checks on new staff and councillors to understand if they are a potential security risk?

Hardware, data, encryption and technology

a) Is backup personal data encrypted?

b) Do you have appropriate mechanisms for securely sending files?
c) Do you have a list of servers, and individuals who are responsible for ensuring that they are up to date?
d) Do you have appropriate firewalls and intrusion detection software?
e) Are your wireless networks appropriately secured?
f) Do you regularly check the operating systems, data and software against a 'good known state' baseline?
g) Do you review unsuccessful attacks and probes / scans?
h) Do you have an inventory (or list of) hardware and software you use?
i) Do you appropriately limit access to data on a ‘need to know’ basis?
j) Do you back-up personal data on a regular basis?
k) Do you apply regular IT updates to your computer hardware and software?
l) Do you ensure that staff and councillors have anti-virus software loaded and active on their devices at all times?
m) Do you have appropriate policies regarding use of external hard drives or USB drives?
n) Do you conduct regular penetration tests and / or red teaming, with appropriate analysis of results?

Third parties

a) Do you properly understand risks arising from third party service providers?
b) Do you undertake due diligence before engaging third party service providers?
c) Do you assess third parties for cyber security or data protection risks?
d) Do you have obligations in your contracts with third parties requiring them to take steps to keep data secure?
e) If you use cloud storage, do you have contractual rights to be notified quickly of potential security issues?

Remote access/BYOD

a) Do you require multifactor authentication where appropriate?
b) Do you allow remote access?
c) If so, do you have the right software and controls in place to ensure it is secure?
d) Do you have policies to secure mobile devices?
e) Is data encrypted on mobile devices?
f) Can mobile devices be remotely wiped? If you use BYOD, do you apply restrictions to maintain security?

User accounts / passwords

a) Do you require unique user accounts?
b) Do you require multifactor authentication where appropriate?
c) Do you restrict administrator accounts to the minimum necessary?
d) Do you require strong, hard to guess, passwords?
e) Do you automatically prevent use of common passwords?