FAIRFIELD TOWNSHIP
RESOLUTION NO. 26-58

RESOLUTION AUTHORIZING THE TOWNSHIP ADMINISTRATOR TO EXECUTE ALL NECESSARY DOCUMENTS TO RENEW THE TOWNSHIP'S COVERAGE FOR CYBER INSURANCE THROUGH CFC, AT AN ANNUAL COST NOT TO EXCEED $8,770.00 EFFECTIVE JUNE 1, 2026, THROUGH MAY 31, 2027.

WHEREAS: Fairfield Township currently has Cyber Coverage and is looking to renew its $1 million policy; and

WHEREAS: Cyber security & ransom threats have continued to increase and pose a serious threat to business; and

NOW, THEREFORE, BE IT RESOLVED, by the Board of Trustees of Fairfield Township, Butler County, Ohio, as follows;

SECTION 1: The Board hereby authorizes the Administrator to sign all necessary documents to renew Cyber Coverage for the Township with CFC at an annual cost not to exceed $8,770.00 for the policy period June 1, 2026, through May 31, 2027, set forth in the attached Exhibit "A".

SECTION 2: The Fiscal Officer is hereby authorized to pay for the premiums of the Cyber Insurance from the following funds: General Fund #1000, Permissive Motor Vehicle License Fund #2231, Police Fund #2018 and Fire Fund #2111.

SECTION 3: The Board hereby dispenses with the requirement that this resolution be read on two separate days, pursuant to RC 504.10, and authorizes the adoption of this resolution upon its first reading.

SECTION 4: This resolution is the subject of the general authority granted to the Board of Trustees through the Ohio Revised Code and not the specific authority granted to the Board of Trustees through the status as a Limited Home Rule Township.

SECTION 5: That it is hereby found and determined that all formal actions of this Board concerning and relating to the passage of this Resolution were taken in meetings open to the public, in compliance with all legal requirements including §121.22 of the Ohio Revised Code.

SECTION 6: This resolution shall take effect at the earliest period allowed by law.

Adopted: June 23, 2026

Board of Trustees	**Vote of Trustees**
Michael Berding:	Yes
Shannon Hartkemeyer:	Yes
Joe McAbee:	Yes

AUTHENTICATION
This is to certify that this is a resolution which was duly passed and filed with the Fairfield Township Fiscal Officer this 23rd day of June, 2026.

ATTEST:

Shelly Schultz, Fairfield Township Fiscal Officer

APPROVED AS TO FORM:

KL Barbiere /LEB

Katherine Barbiere, Township Law Director

Kimberly Lapensee

From: Nadeen Hadadeen <nadeen.hadadeen@onedigital.com>
Sent: Friday, May 15, 2026 1:36 PM
To: Kimberly Lapensee
Cc: French, Dianne
Subject: RE: EFF 06/01/2026 - Package & Cyber renewal - Faitfield Township

Hello Kim, hope all is well!

Pleased to confirm that Fairfield Township is exempt from the surplus line tax on the Cyber Liability policy, and the revised cost will be $8,770.

Please feel free to reach out if you have any questions or concerns.

Wish you a great Weekend!

Best regards,
Nadeen

Nadeen Hadadeen, RPLU
Client Relations Manager | OneDigital
513-644-1283 | Cincinnati, OH

From: Nadeen Hadadeen
Sent: Thursday, May 14, 2026 1:24 PM
To: Kimberly Lapensee <klapensee@fairfieldtwp.org>
Cc: French, Dianne <dfrench@fairfieldtwp.org>
Subject: EFF 06/01/2026 - Package & Cyber renewal - Faitfield Township

Hi Kim, hope all is well!

Please see the attached revised quote, along with the breakout for the PKG policy through OTARMA, updated to include the 2025 Milton Street property at a total insured value of $350,000.

I have also attached the updated summary sheet, which now reflects the Cyber Liability renewal effective June 1, 2026. Key highlights:

- **Overall Limit:** $1,000,000

- **Deductible:** $10,000 (aggregate)
- **Total Cost (2026):** $9,196 (including taxes and fees)
- **Total Cost (2025):** $10,434

Please note this policy is placed with a non-admitted carrier (Underwriters at Lloyd's of London). As required by Ohio law, a few items will be needed:

1. A signed surplus lines disclosure form prior to binding
2. A signed application form within 14 days
3. Downloading and registering the CFC cyber incident response app within 30 days (see attached flyer)

Separately, I'm looking into whether a tax exemption may apply to the $426 Ohio surplus lines tax and will follow up once I have a confirmed answer from legal counsel.

Once you've had a chance to review, please don't hesitate to reach out with any questions.

Best regards,
Nadeen

Nadeen Hadadeen, RPLU
Client Relations Manager | OneDigital
513-644-1283 | Cincinnati, OH

Kimberly Lapensee

From: Nadeen Hadadeen <nadeen.hadadeen@onedigital.com>
Sent: Thursday, May 14, 2026 1:24 PM
To: Kimberly Lapensee
Cc: French, Dianne
Subject: EFF 06/01/2026 - Package & Cyber renewal - Faitfield Township
Attachments: Fairfield Township, .R0404PC2026-1_quote_proposal.pdf; Fairfield Township, .Breakout Report.R0404PC2026-1.pdf; Summary of Insurance 2026-2027 (FAIRTOW-03).xlsx; CFC Cyber Response App Flyer US.PDF.pdf; Renewal Invite ESN0340384420 03 March 2026 cybersecurity.pdf

Hi Kim, hope all is well!

Please see the attached revised quote, along with the breakout for the PKG policy through OTARMA, updated to include the 2025 Milton Street property at a total insured value of $350,000.

I have also attached the updated summary sheet, which now reflects the Cyber Liability renewal effective June 1, 2026. Key highlights:

- **Overall Limit:** $1,000,000
- **Deductible:** $10,000 (aggregate)
- **Total Cost (2026):** $9,196 (including taxes and fees)
- **Total Cost (2025):** $10,434

Please note this policy is placed with a non-admitted carrier (Underwriters at Lloyd's of London). As required by Ohio law, a few items will be needed:

1. A signed surplus lines disclosure form prior to binding
2. A signed application form within 14 days
3. Downloading and registering the CFC cyber incident response app within 30 days (see attached flyer)

Separately, I'm looking into whether a tax exemption may apply to the $426 Ohio surplus lines tax and will follow up once I have a confirmed answer from legal counsel.

Once you've had a chance to review, please don't hesitate to reach out with any questions.

Best regards,
Nadeen

Nadeen Hadadeen, RPLU
Client Relations Manager | OneDigital
513-644-1283 | Cincinnati, OH

ONEDIGITAL
INSURANCE | FINANCIAL SERVICES | HR CONSULTING

ONEDIGITAL | Coverage Details – Fairfield Township Cyber Policy			
#	Coverage / Section	Limit	Notes
Insuring Clause 1: Cyber Incident Response			
A	Incident Response Costs	$1,000,000 / claim	
B	Legal & Regulatory Costs	$1,000,000 / claim	
C	IT Security & Forensic Costs	$1,000,000 / claim	
D	Crisis Management Costs	$1,000,000 / claim	*RT Specialty enhanced wording*
E	Privacy Breach Management Costs	$1,000,000 / claim	*Notifications, credit monitoring, call center*
F	3rd Party Privacy Breach Mgmt	$1,000,000 / claim	
G	Post Breach Remediation Costs	$75,000 / claim	★ *Enhanced by RT Specialty (base $50K)*
Insuring Clause 2: Cyber Crime			
A	Funds Transfer Fraud	$250,000 / claim	
B	Invoice Manipulation	$250,000 / claim	
C	New Vendor Fraud	$250,000 / claim	
D	Physical Goods Fraud	$250,000 / claim	
E	Theft of Personal Funds	$250,000 / claim	
F	Corporate Identity Theft	$250,000 / claim	
G	Theft of Funds Held in Escrow	$250,000 / claim	
H	Theft of Client Funds	$50,000 / claim	
I	Customer Payment Fraud	$50,000 / claim	
J	Telephone Hacking	$250,000 / claim	
K	Unauthorized Use of Computer Resources	$250,000 / claim	
Insuraing Clause 3: Cyber Extortion			
	Extortion / Ransom (incl. cryptocurrency)	$1,000,000 / claim	*Covers fiat, crypto & tangible property ransoms*
Insuring Clause 4: System Damage & Business Interruption			
A	System Damage & Rectification Costs	$1,000,000 / claim	
B	Hardware Replacement Costs	$1,000,000 / claim	
C	Income Loss & Extra Expense	$1,000,000 / claim	*Triggers after 6-hour time franchise*
D	Emergency & Continuity Costs	$100,000 / claim	
E	Voluntary & Regulatory Shutdown	$1,000,000 / claim	
F	Dependent Business Interruption	$1,000,000 / claim	
G	Consequential Reputational Harm	$1,000,000 / claim	*12-month indemnity period*
H	Lost or Missed Bids	$1,000,000 / claim	
I	Claim Preparation Costs	$50,000 / claim	★ *Enhanced by RT Specialty (base $25K)*
★	Non-Tech Dependent BI	$1,000,000 / claim	★ *RT Specialty addition – non-tech vendor outage*
★	Contingent Property Damage	$250,000 / claim	★ *RT Specialty addition – cyber-caused property damage*
Insuring Clause 5: Network Security & Privacy Liability			
A	Network Security Liability	$1,000,000 aggregate	*Incl. costs & expenses*
B	Privacy Liability	$1,000,000 aggregate	*Incl. costs & expenses*
C	Management Liability	$1,000,000 aggregate	*Incl. costs & expenses*
D	Regulatory Fines, Penalties & Investigations	$1,000,000 aggregate	*Insurability per most favorable state law*
E	PCI Fines, Penalties & Assessments	$1,000,000 aggregate	*Incl. fraud recoveries & card reissuance*
F	Contingent Bodily Injury	$250,000 aggregate	*Incl. costs & expenses*
★	Corrective Action Plan Costs (HIPAA)	$50,000 aggregate	★ *RT Specialty addition*
★	Wrongful Collection & Use of Personal Data	$50,000 aggregate	★ *RT Specialty addition*
★	Data Privacy Regulatory Investigation	$50,000 aggregate	★ *RT Specialty addition*
Insuring Clause 6: Criminal Reward Cover			
	Criminal Reward Cover	$100,000 / claim	
Insuring Clause 7: Media Liability			
A	Defamation	$1,000,000 aggregate	*Incl. AI-generated content*
B	IP Rights Infringement	$1,000,000 aggregate	*Covers trade secrets, copyright, trademark; incl. AI*
Insuring Clause 8: Technology E&O			
	Technology Errors & Omissions	⛔ NO COVER	*Excluded from this policy*

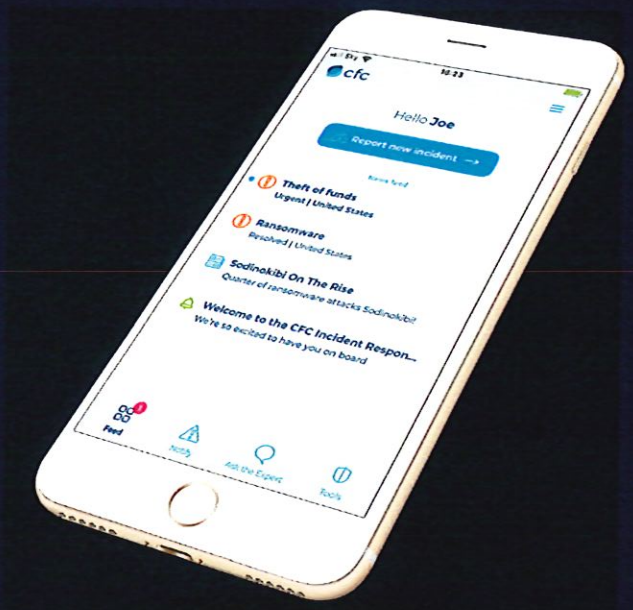
Insuring Clause 9: Court Attengance Cost		
Court Attendance Costs	**$1,000,000 aggregate**	★ *Enhanced (base $100K); $3,000/day sub-limit*
Premium: $9,196 including taxes and fees		

★★★★★
Best Customer App
Insurance Times Tech & Innovation Awards

cfc

Response

An integral part of our cyber policy, our award-winning mobile app Response, delivers critical cyber security alerts and expert support



Here's what this valuable tool has to offer:

Critical threat alerts

Delivered in real-time, CFC alerts customers to cyber threats targeting their business, helping to prevent attacks before they happen.

Expert technical support

The app offers a direct, secure way of communicating with CFC's expert cyber security team to remediate vulnerabilities or seek technical support.

Report an incident

If an incident occurs, the app is the quickest way to notify CFC and receive immediate support from our expert response team, who will help triage the issue and mitigate the impact.

Access to cyber security tools

Designed to keep customers secure, including dark web monitoring, phishing simulations, and deep scanning. These tools are available for free with just a click of a button.

Search CFC Response in the App Store or Google Play store.
Use DEMOCFC000 to sign up.

Download on the App Store | GET IT ON Google Play

Cyber private enterprise
Renewal application form

US

Basic company details

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy. Any defined terms will be bolded and highlighted in blue and can be found in the glossary at the end of this application form:

Company name: Fairfield Township

CFC policy number:

Primary address (address, state, ZIP, country): 6032 Morris Road, Hamilton, Ohio 45011

Description of business activities: Government

Website address: www.fairfieldtwp.org

Date established (MM/DD/YYYY): 01/01/1794

Number of employees: 112

Last 12 months gross revenue: $ 16,219,016.81

Revenue from international sales (%):

Last 12 months gross profit: $ 0.00

Please state which financial institution(s) you use for your commercial banking:

Huntington Bank

Primary contact details

Please provide contact details for the individual within your organization who is primarily responsible for IT security. These details will be used to provide information about downloading our incident response app and receiving risk management alerts and updates:

Contact name: Chuck Goins

Position: Assistant Township Administrator

Email address: cgoins@fairfieldtwp.org

Telephone number: 513887-4400

Previous cyber incidents

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

☐ Cyber extortion ☐ Data loss ☐ Denial of service attack ☐ IP infringement

☐ Malware infection ☐ Privacy breach ☐ Ransomware ☐ Theft of funds

☐ Other (please specify)

If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? ☐ Yes ☐ No

If 'yes', please provide more information below, including details of the financial impact and measures taken to prevent the incident from occuring again:

Revenue analysis

Please provide the following details for your top 5 clients:

Name of client:	Primary services:	Annual revenue derived from client:
Butler County Auditors Office	Collection of Taxes	$ 11,450,978.44
State of Ohio	Rollback Taxes	$ 725,447.24
City of Hamilton	JEDD payments	$ 690,898.64
Medicount	EMS Billing	$ 920,775.61
Huntington Bank	Interest Earned on Invest	$ 572,415.00

IT infrastructure and resourcing

Please confirm the name of your managed service provider (if applicable): SWOCA

What is the approximate number of servers on your network? 7

What is the approximate number of desktops and laptops on your network? 175

What is your annual IT budget? $ 325,000.00

What approximate percentage of your IT budget is spent on IT security?

Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? ☑ Yes ☐ No

If you answered "yes" to the question above, please list your critical third party technology providers below (up to a maximum of 10), including a brief summary of the technology services they provide for you:

SWOCA operates as our contracted IT service department. They provide Internet services with managed firewall, CyberSecurity training, Virtual server services, and IT support.

Data storage and management

Please provide the approximate number of unique individuals that you collect, store and/or process personally identifiable information from, whether on your own systems or with third parties:

Data type	Number of unique individuals
Sensitive data (e.g. medical records, passport details, social security numbers etc):	
Non-sensitive data (e.g. full names, addresses, email addresses etc):	

Please describe your approach towards protecting sensitive and confidential information (e.g. access controls, encryption, network segmentation etc):

SWOCA Deploys Network Segmentation between township departments. All remote access requires MFA, as does desktop access for some departments (based on department level policy.)

Please provide details of how often you purge records that are no longer required:

Please provide details on how you store your back-ups of critical data (e.g. online back-ups stored on your organization's live environment, offline back-ups stored on a removable storage device that is fully disconnected and inaccessible from the live environment, back-ups stored with an online cloud storage provider etc.):

SWOCA's hosted virtual server service includes a 3-2-1 backup structure, with data replicated daily to our on-Net DR site, and immutable copies.

Please provide details on the frequency of your back-ups, including the frequency of full system back-ups and the frequency of incremental/ differential back-ups of critical data:

Daily snapshots, weekly Full backups.

Please provide details on how you secure your back-ups (e.g. back-ups are disconnected and inaccessible from the live environment, multi-factor authentication is required for access to cloud back-ups etc):

We do not use cloud services for backup. Our backup appliance is not accessible from the live environment, and only accessible to limited SWOCA Staff. All remote access requires MFA, and on-site access is only permitted from a secure environment.

Please provide details on how you test your back-ups, including details on how frequently you test the full restoration and recovery of key server configurations and data from back-ups:

Backup restores are tested monthly.

Please provide details on the number of back-up copies you take, including details on how you prevent separate back-up copies being impacted by the same event (if applicable):

We maintain at least three copies of data in two seperate data centers, and the backup appliance inforces immutable backup copies. The data centers are geogrpahicaly diverse, and the off-site data center is only accessible by key workstations within the SWOCA network.

Endpoint security

Which endpoint protection product do you use on your network?
Please provide the name of the vendor and the product used: Sophos XRD

Do you use an endpoint detection and response (EDR) product on your network? ☑ Yes ☐ No

If "yes":

Which product do you use: FortiEDR with FortiSEIM

Please provide an overview of how your EDR product is monitored and managed (e.g. internal IT team or outsourced to a third party):

SWOCA manages a Sophos XDR deployment for the Township, in addition to an emergnging Network level FortiEDR deployment.

Is the EDR product deployed on all endpoints on your network? ☑ Yes ☐ No

If "no":

What percentage of endpoints do not have EDR deployed and why is it not deployed on these endpoints:

Perimeter security

Do you have next-generation firewalls deployed at all network ingress/egress points? ☑ Yes ☐ No

How often do you conduct vulnerability scanning of your network perimeter? Weekly

How often do you conduct penetration testing of your network architecture? Annually

Please provide details of the third party providers you use to conduct penetration testing (if applicable):

Please confirm whether multi-factor authentication is required for *all remote access to your network*: ☑ Yes ☐ No

If you use an alternative method for securing remote access to your network, such as certificate based authentication for devices, please provide details here:

Please confirm whether multi-factor authentication is required to access *all cloud resources holding sensitive or confidential information:* ☐ Yes ☐ No

Email security

Please confirm that multi-factor authentication is enabled for remote access to *all company email accounts:* ☐ Yes ☑ No

Do you simulate phishing attacks to test employees at least annually? ☑ Yes ☐ No

Do you use email filtering software to scan all inbound and outbound email messages in order to filter out spam and malicious content? ☑ Yes ☐ No

If you answered "yes" to the previous question, please state the name of the vendor and product used for email filtering: FortiMail Gateway/Workspace

If you are an Office 365 user, please provide your Microsoft Secure Score
(administrators can find the score using the following link https://security.microsoft.com/securescore):

Network security

Please provide details on how you protect privileged user accounts (e.g. using privileged access management solutions, restricting privileged user accounts to specific devices, enhanced monitoring of accounts for anomalous usage, multifactor authentication enabled for remote access etc):

App privileged accounts require access from either a trusted phyusical environment, or MFA.

Do non-IT users have local administrator rights on their laptops/desktops? ☐ Yes ☑ No

Do you use a network monitoring solution to alert your organization to suspicious activity or malicious behavior on your network? ☑ Yes ☐ No

If you answered "yes" to the previous question, please state the name of the vendor and product used for network monitoring: Solar Winds NPM and FortiSiem/SOAR

Please provide details on whether you have a Security Operations Centre (SOC) that is responsible for event monitoring and detection, vulnerability management and incident response. Please include details on the hours of operation and whether this is an internal function or outsourced to a third party:

SWOCA's SOC operates 8-4 PM M-F,and is backed up by Agile Blue 24/7 SOC as a service.

Do you have any end of life or end of support software? ☐ Yes ☑ No

If "yes", please provide details on what the end of life or end of support software is, how it is used, whether it is segregated from the rest of the network and if so, how it is segregated:

Please describe your patch management process and how you ensure that all critical patches are applied in a timely fashion, including a timeframe of how quickly you would implement patches for zero day vulnerabilities after they have been released by the vendor:

Monthly patch maintenance window with a focus on depllying patches within 48 hours of release, 24 hours for any Critial or HIGH ranked vulnerabilities.

Please provide details of any major changes that you have planned for your IT infrastructure in the next 12 months (if any):

Additional controls

Please confirm that **before** any change is made to a third party's account details, you obtain authorization from the third party via an authentication method which is different to the original method used to request the change? ☑ Yes ☐ No

Please confirm that **before** you transfer funds to an account that you haven't paid into before, you obtain authorization from the recipient of the funds via an authentication method which is different to the original method used to request the transfer? ☐ Yes ☐ No

Do you provide training on phishing/social engineering scams for all employees involved in transferring funds on behalf of your organization on at least an annual basis? ☑ Yes ☐ No

Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

☑ Application whitelisting	☑ Asset inventory	☑ Custom threat intelligence	☑ Database encryption
☑ Data loss prevention	☑ DDoS mitigation	☑ DMARC	☑ DNS filtering
☑ Employee awareness training	☑ Incident response plan	☑ Intrusion detection system	☑ Perimeter firewalls
☑ Security info & event management	☑ Virtual private network (VPN)	☑ Web application firewall	☑ Web content filtering

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

FortiGuard, FortiEDR, Sophos XDR, FortiSiem, ForiClient EMS, Windows Group Policy, Fortinet Security Awarness Training, TechGuard

Important notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. CFC Underwriting will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on our privacy policy please visit ***www.cfcunderwriting.com/privacy***

Contact name: KIMBERLY VAPENSEE Position: TOWNSHIP ADMINISTRATOR

Signature: Kimberly Vapensee Date (MM/DD/YYYY): 5/15/26

Glossary of terms

Application whitelisting
A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset inventory
A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence
The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organizations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption
Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention
Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation
Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC
An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering
A specific technique to block access to known bad IP addresses by users on your network.

Email filtering
Software used to scan an organization's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

Employee awareness
Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

Endpoint detection and response (EDR)
A software tool that works by monitoring and collecting data from endpoints and recording the information in a central database where further analysis, detection, investigation, reporting and alerting take place.

Endpoint protection
Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

Incident response plan
Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system
A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Managed service provider
A third party organization that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Mobile device encryption
Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Multi-factor authentication
Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network monitoring
A system, utilizing software, hardware or a combination of the two, that constantly monitors an organization's network for performance and security issues.

Next-generation firewalls
Software or hardware solutions that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems and anti-virus.

Penetration tests
Authorized simulated attacks against an organization to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls
Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)
System used to aggregate, correlate and analyze network security information – including messages, logs and alerts – generated by different security solutions across a network.

Security Operations Centre (SOC)
A facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. SOC's can be internal and run by the organization themselves or outsourced to a third party.

Virtual private network (VPN)
A VPN is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. Most commonly used to provide a secure remote connection to an organization's network.

Vulnerability scans
Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall
Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering
The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organization. For example, known malicious websites are typically blocked through some form of web content filtering.