

Document Title	ShieldNet Cybersecurity Core Training Syllabus
Release Date	April 2026
Version	1.0

Universal Literacy For Everyone

ShieldNet Core Training is a free, self-paced cybersecurity literacy program designed for everyone any age, any role, any level of technical background. It is not a framework course. It is a practical education in how digital threats work, how to defend against them, and how to behave securely in personal and professional life. The ShieldNet Cybersecurity Standard appears as a thread throughout and is introduced fully in the final bridge module.

Audience	Everyone - no prerequisites, no technical background required
Total Modules	21 content modules + Module 0 (orientation) + Module 21 (ShieldNet bridge)
Content duration	~3.5 hours across 22 modules
Structure	5 thematic parts, each with a central idea and identity
Module format	Real-world opener · Concept sections · ShieldNet thread · Summary · 4 practice questions
Practice questions	4 per module · 80 total · scenario-based · formative
Final Assessment	40 scenario-based questions · 60 minutes · 75% pass mark
Credential	Digital badge via Certifier.io · completion certificate · training record
ShieldNet gateway	Core Training completion is mandatory before Implementor or Auditor pathways

Orientation

Welcome

Module 0

M0	**Welcome and Orientation** *How to use this course and what to expect* • Navigate the course structure and understand how parts and modules connect • Understand the assessment format and what the final badge recognizes • Know where ShieldNet appears throughout the course and why it is designed the way it is

ShieldNet Cybersecurity Core Training Syllabus © 2026 by IS Consulting is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

Part 1

Understanding the Digital World

Modules 1-3

M1	**Your Digital Life** *Data, devices and why attackers want them* • Explain what personal and organizational digital assets are and why they have value • Describe how data ends up on the dark web and how credential stuffing works • Counter the 'I have nothing to hide' argument with specific examples • Use haveibeenpwned.com to check whether your email has appeared in a breach
M2	**Confidentiality, Integrity, Availability** *The three things worth protecting* • Define confidentiality, integrity and availability in plain language • Give a real-world example of each principle being violated • Explain why availability matters even when no data is stolen • Describe a scenario where all three principles are broken simultaneously
M3	**Risk** *What it is, why we can't eliminate it, and how we think about it* • Explain the difference between a threat, a vulnerability, and a risk • Describe how likelihood and impact combine to determine risk priority • Name the four ways an organization can respond to a risk, with an example of each • Explain why zero risk is not the goal of security

Part 2

Know Your Enemies: How Attacks Actually Work

Modules 4-8

M4	**Phishing and Social Engineering** *Hacking humans* • Describe how a phishing attack works and why urgency is the attacker's most powerful tool • Identify at least five red flags in a suspicious email • Explain the difference between phishing, smishing, and vishing • State the three-step response to a suspicious message: stop, check, report
M5	**Malware** *When software becomes a weapon* • Name four types of malware and describe what each one does • Explain how ransomware works from initial entry to ransom demand • Describe the 3-2-1 backup rule and why the offline copy is the critical element • Identify three specific actions to reduce personal exposure to malware

ShieldNet Cybersecurity Core Training Syllabus © 2026 by IS Consulting is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

M6	**Passwords and Account Takeover** *The keys to your kingdom* • Explain what credential stuffing is and why password reuse enables it • Describe the difference between a weak and a strong password with examples • Explain what a password manager is and why it is the practical solution • Describe how MFA limits damage even when a password has been stolen
M7	**Networks and the Internet** *How data travels and where it can go wrong* • Explain in plain language what an IP address and DNS are • Describe what a man-in-the-middle attack is and how HTTPS protects against it • Explain two specific risks of public Wi-Fi and one defense for each • Describe what a VPN does and what it does not protect against
M8	**Who Are the Attackers?** *Motivations, targets and methods* • Name four types of attacker and describe their primary motivation and methods • Explain the difference between opportunistic and targeted attacks • Describe what an insider threat is and why it is difficult to defend against • Explain what a supply chain attack is with a real example

Part 3

Build Your Defenses: Practical Protection

Modules 9-14

M9	**Strong Authentication** *Proving who you are* • Explain the three authentication factors and give an example of each • Describe how an authenticator app works and why it is stronger than SMS codes • Explain what MFA fatigue is and how to protect against it • List the accounts where MFA should be enabled as a critical priority
M10	**Controlling Access** *Who gets in, what they can do* • Explain the difference between authentication and authorization • Define the principle of least privilege and give a practical example • Describe three common over-permission patterns and why each creates risk • Explain why dormant accounts belonging to leavers are a security risk

ShieldNet Cybersecurity Core Training Syllabus © 2026 by IS Consulting is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

M11	**Keeping Devices Safe** *Updates, locks and good habits* • Explain why software updates matter for security and what end-of-life software means • List the six key device protection measures and how to verify each one • Explain what full-disk encryption does and why it matters for lost or stolen devices • Describe the risks of using personal devices for work and two mitigations
M12	**Encryption** *Scrambling data so only the right people can read it* • Explain what encryption does using a plain-language analogy • Describe the difference between encryption in transit and at rest • Explain what end-to-end encryption means and why it offers stronger privacy • Describe what key management means and why storing a key with the data defeats encryption
M13	**Your Data and Privacy** *What you share, with whom, and why it matters* • Define personal data and explain why behavioral data is sensitive even when trivial • Explain the free-product business model and what users provide in exchange • Name three rights individuals have under GDPR and describe how to exercise one • Describe two specific steps to reduce data collection in personal digital life
M14	**Trusting Third Parties** *Apps, services and the supply chain* • Explain why installing an app from an official store does not guarantee it is safe • List four questions to ask when evaluating whether to trust a new app • Explain why browser extensions are a higher-risk category of third-party tool • Name two actions to take when you stop using a service or app

Part 4

When Things Go Wrong: Responding and Recovering

Modules 15-17

M15	**Spotting and Reporting Incidents** *Your early warning role* • Define a security incident and give three examples that are often under-reported • Explain why early reporting matters more than certainty about what happened • Describe five warning signs that a security incident may be in progress • Explain why you should disconnect a device from the network rather than shut it down during a suspected ransomware attack

ShieldNet Cybersecurity Core Training Syllabus © 2026 by IS Consulting is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

M16	**Backups and Recovery** *Why 'it's saved' is never enough* • Explain the 3-2-1 backup rule and what qualifies as the offline copy • Name three ways a backup can fail when needed most, with a prevention for each • Define Recovery Point Objective and Recovery Time Objective in plain language • Explain why testing backups is as important as taking them
M17	**Data Breaches** *What happens, what it means, what you do* • Define a personal data breach and explain the three types using the CIA triad • State the two GDPR notification obligations and the key thresholds and timelines • Describe five steps an individual should take when their credentials are breached • Explain why documenting a breach matters even below the notification threshold

Part 5

Security as a Mindset: Habits, Culture and Staying Current

Modules 18-20

M18	**Safe Digital Habits** *The small things that make a big difference* • Explain why security habits are more valuable than security knowledge not acted on • Describe the one-second rule and what it protects against • Define shadow IT and give two examples of how it creates risk • Describe three specific steps in a social media security audit
M19	**Security Is Everyone's Job** *Your role in a safer organization* • Explain why security teams cannot protect an organization alone • Describe two specific security responsibilities that apply to every staff member • Explain what a security culture is and two observable signs that distinguish strong from weak • Explain what a security champion does and one action they might take
M20	**Staying Ahead** *How security evolves and how you keep up* • Explain what stays constant in cybersecurity even as specific threats change • Name two authoritative sources of free security information and what each provides • Explain how AI is changing the phishing threat and one defense that remains effective • Describe what Ransomware as a Service means and why it increases attack volume

ShieldNet Cybersecurity Core Training Syllabus © 2026 by IS Consulting is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/

Bridge Module

From Concepts to Practice: A First Look at ShieldNet

Module 21

M21	**From Concepts to Practice: A First Look at ShieldNet** *The bridge between this course and the ShieldNet Standard* • The five Action Zones and their canonical taglines • How all 20 content modules map to specific ShieldNet Core Standard controls • The structure of a ShieldNet control (control text, Why, evidence examples, legal anchors) • The Annex A templates and which controls they evidence • What ShieldNet looks like in practice for small and medium organizations • The EU regulatory landscape: NIS2, GDPR, and the Cyber Resilience Act

Final Assessment

Format	40 scenario-based multiple-choice questions
Time allowance	60 minutes
Pass mark	75% (30 of 40 questions correct)
Question style	Applied judgement and contextual understanding, not recall of framework terminology or control identifiers
Question distribution	Drawn from all five parts; weighted towards Parts 2 and 3 (threat recognition and practical defense)
Credential on passing	Digital badge via Certifier.io · completion certificate · training record stored in ShieldNet Training Database
Prerequisite for	Implementor Professional Training · Auditor Professional Training

ShieldNet Cybersecurity Core Training Syllabus © 2026 by IS Consulting is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/