# Employee Technology Usage & Cybersecurity Awareness Survey

*This survey is anonymous and aims to improve technology support, security practices, and regulatory compliance across the organization. Your honest input helps us provide safer, more effective tools and processes.*

## Section 1: General Information

1. **What is your current job role?**
   * IT
   * OT
   * Cybersecurity Specialist
   * Manufacturing/Production
   * Engineering/Maintenance
   * Management
   * Admin/Support Services
   * Other: \_\_\_\_\_\_\_\_\_\_\_\_
2. **Which department/Area do you primarily work in?**
   * IT Security
   * IT Operations
   * Networking
   * IT Audit
   * Quality
   * HR
   * Finance
   * Other: \_\_\_\_\_\_\_\_\_\_\_\_
3. **Length of time with the organization:**
   * Less than 1 year
   * 1–5 years
   * 6–10 years
   * Over 10 years

## Section 2: Official Technology Use

1. **Please list the main software or Hardware officially provided by the company for your work tasks:**
   * E.g. Nmap, SolarWinds, Datadog etc
2. **How satisfied are you with the tools officially provided?**
   * Extremely satisfied
   * Satisfied
   * Neutral
   * Dissatisfied
   * Very dissatisfied
3. **Do the provided tools meet your daily work needs?**
   * Always
   * Most of the time
   * Sometimes
   * Rarely
   * Never
4. **Has the company asked for your feedback on technology solutions?**
   * Yes, regularly
   * Occasionally
   * Rarely
   * Never

## Section 3: Use of Additional or Unofficial Technology

1. **Have you used any additional tools or devices (Hardware or Software) not formally approved by the company to help you complete work?**
   * Yes
   * No
   * Prefer not to answer
2. **Which types of additional tools have you used? (Select all that apply):**
   * Cloud storage (e.g., Google Drive, Dropbox)
   * Collaboration apps (e.g., Slack, Trello, Notion)
   * Personal devices (smartphones, laptops, tablets)
   * Remote access software (e.g., TeamViewer)
   * IoT/IIoT devices or sensors
   * AI tools (e.g., ChatGPT, Bard)
   * Data analytics/visualization software
   * Other: \_\_\_\_\_\_\_\_\_\_\_\_
3. **Why did you choose to use additional tools? (Select all that apply):**

* Company tools were too slow/incomplete
* Needed something easier/faster to use
* For personal productivity
* Cost-effective
* Recommended by others
* Didn’t realize it required approval
* Other: \_\_\_\_\_\_\_\_\_\_\_\_

1. **Would you prefer to use only approved tools if they met all your needs?**

* Definitely
* Probably
* Not sure
* Probably not
* Definitely not

1. **Have you ever suggested a new tool or system to your manager or IT?**

* Yes, approved
* Yes, denied
* Yes, still pending
* No

1. **Please list additional tools or devices (Hardware or Software) not formally approved by the company but you use sometimes help you complete work?**
   1. E.g. Lansweeper
   2. E.g. Wireshark
   3. E.g. Zabbbix

## Section 4: Cybersecurity and Risk Awareness

1. **How concerned are you about cybersecurity threats in your role?**

* Extremely concerned
* Somewhat concerned
* Slightly concerned
* Not concerned

1. **Do you feel confident identifying cyber threats (e.g., phishing, suspicious files, malicious links)?**

* Very confident
* Somewhat confident
* Slightly confident
* Not confident

1. **Have you received formal cybersecurity training in your current role?**

* Yes, in-depth training
* Basic training
* No training
* Not sure

1. **Are you aware of how to report suspicious emails or security issues?**

* Yes
* Somewhat
* No

## Section 5: Ransomware and Phishing Awareness

1. **Have you received suspicious emails that you believed could be phishing?**

* Yes, frequently
* Yes, occasionally
* No
* Unsure

1. **Have you ever accidentally clicked a suspicious link or attachment?**

* Yes
* No
* Not sure

1. **Has your organization experienced a ransomware or phishing incident you were aware of?**

* Yes, personally affected
* Yes, heard internally
* No
* Not sure

1. **Has the organization provided clear guidelines on responding to phishing or ransomware threats?**

* Very clear
* Somewhat clear
* Not clear
* No guidance provided

1. **How confident are you that your organization is actively defending against cyber threats?**

* Very confident
* Somewhat confident
* Slightly confident
* Not confident

## Section 6: Real-World Case Awareness

1. **Are you aware of any of the following cybersecurity incidents? (Select all that apply):**

* **HSE (Ireland, 2021)** – Ransomware via phishing and outdated email servers
* **Quanta Computer (Taiwan, 2021)** – Attack through unauthorized remote access tools
* **Leoni AG (Germany, 2022)** – Disruption from legacy systems and insecure third-party tools
* None of the above
* Not sure

1. **Do you believe similar risks (e.g., third-party tools, outdated systems, remote access) could exist in your workplace?**

* Definitely
* Possibly
* Unlikely
* No
* Not sure

1. **What do you see as the greatest cybersecurity risks in your work environment? (Select up to 3):**

* Outdated software/hardware
* Third-party or contractor access
* Unofficial tools or apps
* Poor training or awareness
* Weak password/security policies
* Inadequate monitoring/visibility
* Other: \_\_\_\_\_\_\_\_\_\_\_\_

## Section 7: Data Protection and GDPR Compliance

1. **Do you handle any personal or sensitive data (e.g., employee, client, financial)?**

* Yes, regularly
* Occasionally
* No
* Not sure

1. **How confident are you that you manage this data in compliance with privacy regulations (e.g., GDPR)?**

* Very confident
* Somewhat confident
* Slightly confident
* Not confident

1. **Have you received training specifically about GDPR or data privacy policies?**

* Yes, comprehensive
* Yes, basic
* No
* Unsure

1. **Have you ever stored or shared sensitive data using unofficial platforms or personal devices?**

* Yes
* No
* Prefer not to answer

1. **Do you know how to report a potential data breach or privacy concern?**

* Yes
* Somewhat
* No

1. **Would additional training on data protection and GDPR help you in your role?**

* Definitely
* Probably
* Not sure
* Not needed

## Section 8: Support, Culture & Improvements

1. **How responsive is IT when you report an issue or request assistance?**

* Very responsive
* Occasionally responsive
* Rarely responsive
* Never contacted IT

1. **Does your team or department actively encourage tech suggestions or feedback?**

* Yes, frequently
* Sometimes
* Rarely
* Not at all

1. **How comfortable are you discussing IT or cybersecurity concerns with management or IT?**

* Very comfortable
* Somewhat comfortable
* Slightly comfortable
* Not comfortable

1. **What would help you use only approved and secure tools at work? (Select up to 3):**

* Faster and easier official tools
* Quicker IT support
* Better communication from IT/security
* Recognition for good practices
* Clearer policies and training
* Involvement in technology selection
* Other: \_\_\_\_\_\_\_\_\_\_\_\_

## Section 9: Final Comments

1. **What support, tools, or training would help you be more effective and secure in your role?**  
   📝 *Open text*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. **Any additional suggestions or concerns about technology, security, or data privacy?**  
   📝 *Open text*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Thank you for your valuable input.**  
Your feedback will help us improve tools, training, and security practices across the organization.