Prevention first:

The employee lifecycle

and the role of the IT admin in each of them

Digital Security
Progress. Protected.

From onboarding to day-to-day work and eventually offboarding, every employee's journey in an organization encompasses distinct phases, each with its unique IT requirements. Whether welcoming new team members, supporting existing staff, or managing departures, the IT team plays a pivotal role in ensuring the organization's seamless and secure operation.

Having a well-defined process or roadmap for the employee lifecycle isn't just a matter of efficiency—it's a powerful preventive measure. By aligning IT processes with best practices, organizations can mitigate risks related to data security, access control, and compliance. This checklist will guide IT specialists through employees' various work-life stages, empowering them to meet their responsibilities and safeguard the organization's digital environment.

How to use this checklist?

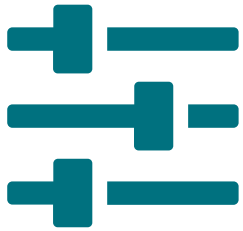
The onboarding and offboarding checklist serves as a reference point for maintaining the safety and efficiency of your digital infrastructure. It will help you consider all the necessary steps for each stage of the employee lifecycle.

Onboarding

Digital Security
Progress. Protected.

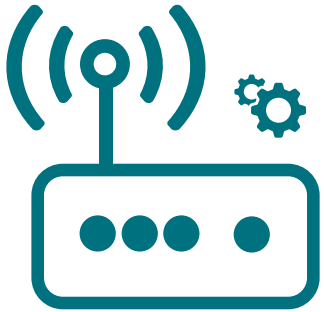
1. Preparing devices for new employees:

- Assign hardware assets and label them accordingly.
- Find all the necessary accessories, including monitors, docking stations, keyboards, and mice.
- Prepare said devices for the new employees. This may involve:
  - ☐ Installing and providing all necessary hardware and software
  - ☐ Configuring email accounts and access permissions
  - ☐ Setting up security measures and user profiles
  - ☐ Customizing the device to align with the user's role and requirements



2. First-day handover:

- Assist the new employees with their first login on-site.
- Help the employees set up their passwords.
- Conduct a device check with the user to ensure everything works properly.
- Provide a basic instruction sheet covering security, Wi-Fi setup, and other essentials.
- Ensure the new employee signs the handover protocol.



3. Regulations and guidelines:

- Share a list and guidelines for the apps and software the employees should use.
- Familiarize your employees with various company policies, including, for instance:
  - ☐ IT/Cybersecurity Policy
  - ☐ GDPR/Data Protection Policy
  - ☐ Remote Working Policy
  - ☐ Social Media Policy
  - ☐ BYOD (Bring Your Own Device) Policy

BYOD (Bring Your Own Device) Policy

The BYOD system is rather popular nowadays, meaning it is necessary to instruct your employees on using their devices for personal and work purposes without endangering your company's security. Here are some issues the BYOD policy should cover:

- ☐ **Who is eligible to participate in the BYOD program**
- ☐ **List of devices, operating systems, and platforms that are allowed and supported under the policy**
- ☐ **Password requirements**
- ☐ **Data encryption requirements**
- ☐ **Remote wipe process explanation**
- ☐ **Data access and usage limitations**
- ☐ **Clarification of the level of IT support provided for personal devices**
- ☐ **Monitoring and auditing specifics**
- ☐ **Employee responsibilities in terms of security and compliance**
- ☐ **What to do in case of a lost or stolen device**
- ☐ **What to do when the employment ends**

Throughout the employment

Digital Security
Progress. Protected.

1. Cybersecurity education:

- Continuously educate employees on cybersecurity threats and best practices.

How to create a cyber-aware culture and avoid security fatigue?

- ☐ Cooperate with the HR department to make the education interactive and useful.
- ☐ Implement shorter, more frequent training sessions, which are often more effective than a single annual training event.
- ☐ Share real-life stories and examples from your experiences to make the content relatable.
- ☐ Utilize fun formats – like games, quizzes, and simulations – to engage employees.
- ☐ You can't make employees more cyber-aware by scaring them. If you use this approach, they will be more likely to fear reporting any mistakes or potential cyber threats.
- ☐ Be open to questions and ensure your employees that you are there to help if they need you.

2. Least privileged access:

- Ensure the principle of least privileged access is followed.
- Regularly review and adjust access permissions accordingly.
- Disable file sharing and email forwarding to external addresses to prevent data leaks.

3. Device maintenance:

- Regularly verify that employees' devices are up-to-date with the latest security patches and software updates. This includes both company-issued and personal devices used for work.

4. Rules for remote work:

- Advise against using personal devices for work tasks – unless your company follows the BYOD system.
- Encourage the use of a Virtual Private Network (VPN) for secure connections.
- Promote the use of encryption for sensitive data.
- Stress the importance of strong Wi-Fi passwords to prevent unauthorized access.
- Ensure endpoint protection is active and up to date on all remote devices.

Offboarding

Digital Security
Progress. Protected.

1. Account and access management:

- Revoke permissions for all applications and services to which the departing employee had access to.
- Reset passwords on all company devices that the employee used.

2. Physical access and hardware:

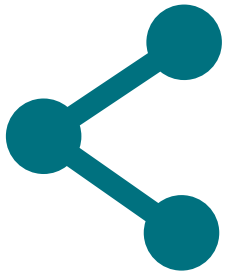
- Revoke building access, including access cards and keys.
- Collect and reclaim all company devices issued to the departing employee, including laptops, smartphones, and other hardware.

3. Monitoring and data protection:

- Maintain regular communication with the departing employee to monitor their behavior during the offboarding process.
- Conduct a final review of monitoring and logging tools to check for any unusual or unauthorized activity associated with the departing employee's accounts and systems.
- Consider deploying a Data Loss Prevention (DLP) solution to uncover unauthorized access to devices or data during or after offboarding.

4. Last day procedures:

- Ensure that hardware handover is completed.
- Block the employee's accounts to prevent further access.
- Perform a secure wipe of the employee's devices to remove company data.



This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach, powered by AI and human expertise.**

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

EXPLORE

Digital Security
Progress. Protected.