Human Resource Management in Information Security

Teng Guo*

School of Cyberspace Security, University of International Relations, Poshang Cun 12, Haidian District, Beijing 100091, China

*guoteng@uir.edu.cn

Abstract. With the rapid development of information technology, information security has become an important mangement project that should be sufficiently emphasized in organizational operations. As is well known, human resource management plays a significant role in information security management. This article aims to explore the key strategies and methods of human resource management to ensure the safety and confidentiality of organizational information assets, ultimately achieving long-term development goals.

Keywords: Information security, Human resource management, Background checks, Safety training and education

1 Introduction

Information security refers to protecting information assets from unauthorized access, use, modification, or destruction etc. Nowadays, information assets have become the core competitiveness of business organizations, and information security management has become the top priority of organizational management. As a core component of information security management, the role of human resource management [1, 2, 3] requires complete understanding and application. In the following, we present a detailed explanation of human resource management in information security.

The core purpose of human resource security management is to define personnel security responsibilities, regulate personnel security behavior, and thus avoid or reduce information security risks caused by personnel factors. This includes the management of internal employees, contractor personnel, and third-party personnel.

The scope of human resource security management includes: (1) Internal employees: A background check of internal employees should be conducted when applying for a position, including the applicant's work ability and personal professional ethics, the completeness and accuracy of their resume, the authenticity of their education and professional qualifications, and identification documents. In addition, for employees who have access to sensitive information, a confidentiality agreement should be signed. Employees who have access to organizational strategic information, core business, research and development, sales and management information should sign a non-compete agreement. (2) Contractors and third-party personnel: The contract with the contractor should clearly specify the responsibilities of the contractor to conduct

D. Hu et al. (eds.), *Proceedings of the 2024 5th International Conference on Modern Education and Information Management (ICMEIM 2024)*, Atlantis Highlights in Social Sciences, Education and Humanities 29,
https://doi.org/10.2991/978-94-6463-568-3_8

personnel background checks on the service personnel dispatched, and be responsible for the results of the background checks. Contractors and third-party personnel should sign confidentiality agreements or information security commitments as a prerequisite for their permission to provide services to the organization and access sensitive information.

The strategies of human resource security management includes: (1) Recruitment and selection: Conduct thorough selection and review of job applicants, especially for key positions who may have extensive exposure to sensitive information. (2) Training and education: Conduct at least one annual comprehensive information security training for all employees, including basic information security knowledge and awareness related to their business. Personnel engaged in information security management and information security technology should participate in at least one specialized information security management training or information security technology and product training related to their work each year. (3) Responsibilities and authorities: The security roles and responsibilities of employees should be described and explained in writing. All personnel's access to information and information processing facilities should be adjusted timely in case of job changes or termination of employment. (4) Contract and legal compliance: Confidentiality agreements or contracts containing confidentiality clauses should undergo compliance review by the legal department before signing to avoid legal and regulatory risks. (5) Performance evaluation and incentives: incorporate new information security into the performance evaluation indicators of departments and employees, moderately reward and implement effectively. See Figure 1.

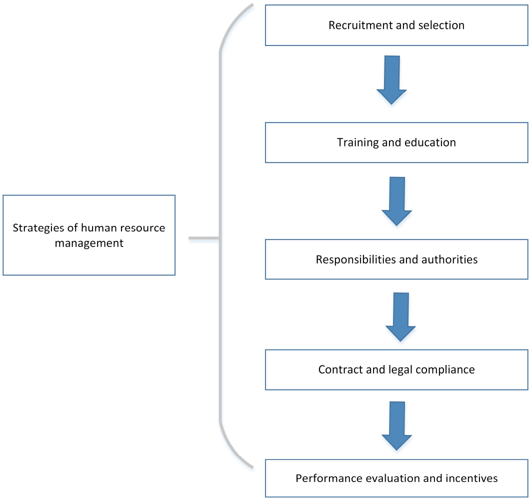
Strategies of human resource management
Recruitment and selection
Training and education
Responsibilities and authorities
Contract and legal compliance
Performance evaluation and incentives

Fig. 1. Five steps of human resource management strategies.

The process of human resource security management includes: (1) Before appointment: Conduct background checks, sign information security responsibility agreements or confidentiality agreements. (2) During employment: Conduct information security education and training to ensure that employees can fulfill their information security responsibilities. (3) Termination or change of appointment: Integrating the protection of organizational interests into the process of personnel change or termination, including information asset recovery, access rights clearance etc.

Overall, human resource management in information security is a comprehensive and systematic process that involves recruitment, training, responsibility and authority management, contract and legal compliance review, and other aspects. By implementing these measures, information security risks caused by personnel factors can be effectively reduced. In the following sections, we will present a detailed analysis of human resource management stage by stage.

2 Recruitment and Selection

In human resource management, recruitment and selection [4, 5, 6] are key steps to ensure that organizations can attract and acquire high-quality talents. The recruitment and selection process includes eight steps, see Figure 2.

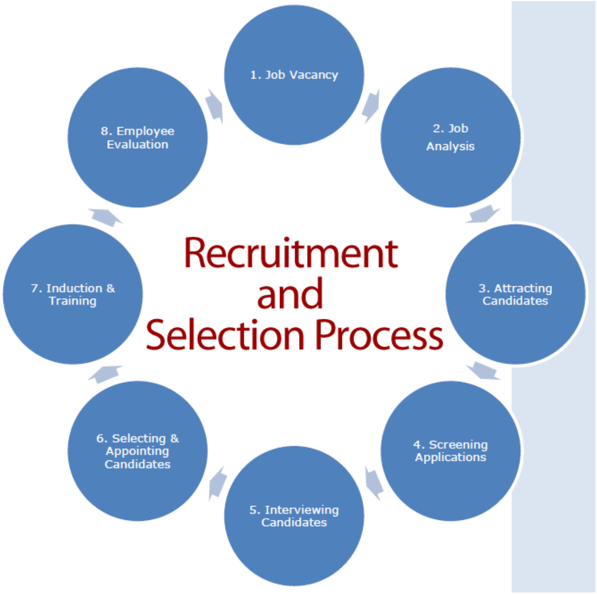
1. Job Vacancy
2. Job Analysis
3. Attracting Candidates
4. Screening Applications
5. Interviewing Candidates
6. Selecting & Appointing Candidates
7. Induction & Training
8. Employee Evaluation
Recruitment and Selection Process

Fig. 2. Eight steps of recruitment and selection process, [Public domain], https://hrmpractice.com/recruitment-and-selection-process.

The following is a detailed analysis of four important aspects of the recruitment and selection of human resource management.

Recruitment is the process by which a company seeks and attracts capable and interested personnel to join the company based on human resource planning and job analysis. In the field of information security management, the main goal of recruitment is to find talents with professional knowledge and skills in information security who are capable of handling information security management problems.

Recruitment process includes: (1) Develop recruitment plan: Clarify recruitment positions, number of personnels, job requirements, etc., providing guidance for subsequent recruitment activities. (2) Posting recruitment information: Publish recruitment information through various channels to attract job applicants. These channels include the company's official website, recruitment websites, social media, etc. (3) Selecting resumes: Select resumes of applicants who meet the requirements of the position, usually by setting keywords related to the position for some quick selection. (4) Interview evaluation: Conduct an interview evaluation on the selected candidates to understand their abilities, experiences, personalities, etc. The interview format can be one-on-one interview, group interview, or video interview, etc. Comprehensive evaluations of applicants can be conducted using assessment tools such as intelligence tests, personality tests, and occupational aptitude tests. Evaluate the adaptability and interpersonal communication ability of job applicants by simulating role interactions in actual work scenarios. (5) Background check: Conduct a background check on qualified applicants to verify whether the information provided is true and reliable. (6) Recruitment Decision: Based on the interview evaluation and background investigation results, make an employment decision and issue a formal employment notice to the applicant.

Selection criteria includes: In the recruitment and selection of information security employees, attention should be paid to the following standards: (1) Professional knowledge and skills: Applicants should have professional knowledge and skills in the field of information security, such as network security, data encryption, risk assessment, etc. (2) Work experience: Applicants with relevant work experience are more likely to be competent in information security management positions because they already have certain practical experience and problem-solving abilities. (3) Communication and collaboration skills: Information security management position requires communication and collaboration with different departments and personnel, so applicants should have good communication and collaboration skills. (4) Sense of responsibility and professionalism: Information security management is crucial for the operation and asset security of an organization, and applicants should have a strong sense of responsibility and professionalism.

Challenges and Countermeasures includes: During the recruitment and selection process, there may be challenges such as difficulty in resume filtering and inaccurate interview evaluations. To address these challenges, the following measures can be taken: (1) Develop clear and scientific recruitment plans and standards to ensure the efficiency and accuracy of the recruitment process. (2) Recruiting through multiple channels to expand the range of candidates. (3) Train interviewers to improve their interview skills and objective evaluation abilities.

Overall, in the recruitment and selection process of human resource management in information security, attention should be paid to standards such as professional knowledge and skills, work experience, communication and collaboration abilities, as well as sense of responsibility and professionalism, and multiple selection methods should be used for a comprehensive evaluation. At the same time, attention should be paid to potential challenges that may arise during the recruitment and selection process, and corresponding measures should be taken to address them.

3 Background Checks

Background checks in human resource management aim at ensuring that hired employees have not engaged in any behavior or background that may pose a threat to the company's information security before joining, see Figure 3. The following is a detailed process and content regarding the background investigation of human resource management in information security management.

The main purpose of background checks is to verify the personal information, educational background, work experience, and other factors that may affect the job performance and security of applicants, in order to ensure that the company hires reliable, honest, and easy to comply with the company's information security policies.

The content of background checks includes: (1) Basic personal information: verify the name, age, ID card number, family background and other basic information of the applicant to ensure that the information provided by the applicant is true and reliable. (2) Education background: Verify the educational background information of applicants, such as their educational background, academic degree, and graduation institution, through official channels to prevent academic fraud. (3) Work experience: Contact the previous employer via phone or email to understand the job performance, reasons for resignation, job responsibilities, and other information of the applicant, ensuring the authenticity and reliability of the applicant's work experience. (4) Bad records: With the candidate's authorization, verify whether the applicant has any negative information such as criminal records, bad credit records, and industry violations through legitimate and compliant official data sources.

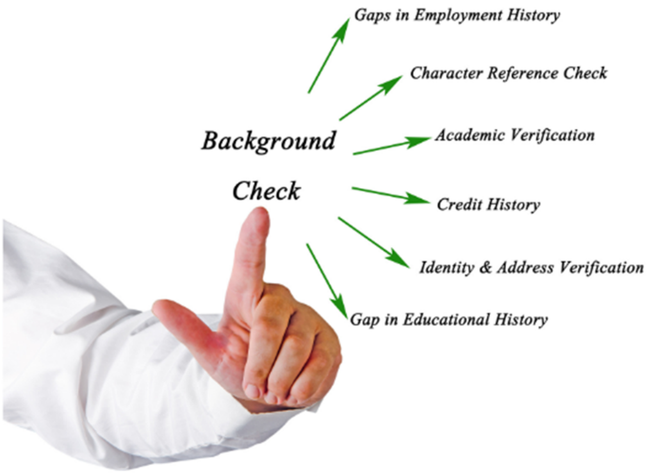
Background
Check
Gaps in Employment History
Character Reference Check
Academic Verification
Credit History
Identity & Address Verification
Gap in Educational History

Fig. 3. Six aspects of background check, [Public domain], https://nnamtique.com/ten-things-background-checks-reveal/background-check-by-canva/.

The method of background checks includes: (1) Online background check: Use databases and online tools to verify the authenticity of the applicant's identity and educational information. (2) Telephone interview: Conduct telephone interviews with former employers or relevant contacts to understand the job applicant's work experience and personal performance. (3) Offline meeting: When necessary, interview former colleagues or leaders of the applicant for face-to-face interviews to obtain more detailed information. (4) Third-party background check: Entrust a professional third-party background check company to conduct background checks, utilizing their rich experience and resources to gain a more comprehensive understanding of the candidate's background information.

The supplements of background checks includes: (1) Legitimacy and privacy protection: When conducting background checks, it is necessary to comply with all applicable laws and regulations, including privacy regulations. Personal information cannot be collected or used without obtaining the applicant's explicit consent. (2) Transparency and open communication: Clearly explain the purpose, scope, and methods of background checks to job applicants, and establish trust relationships. (3) Information accuracy: Ensure the accuracy of the obtained information and avoid relying on a single source of information. (4) Confidentiality: The information obtained from background checks is kept confidential and only shared with those who need to know. (5) Third party background check company selection: If you choose to use a third-party background check company, you should choose a company with good reputation.

Through a strict background check process, it can be ensured that employees hired by the company have not engaged in any behavior or background that may pose a threat to the company's information security before joining. This helps the company reduce information security risks, improve team efficiency, and increase employee’s satisfaction. At the same time, background checks are also an important part of human resources recruitment, which can help companies filter out truly suitable employees and improve overall organizational performance.

4 Safety Training and Education

In information security management, safety training and education [7, 8] in human resource management aim at improving employee security awareness and skills and reducing information security risks. The following are detailed contents and suggestions regarding safety training and education.

The information security awareness and skills of employees are directly related to the security level of enterprise information assets. Strengthening security training and education is a necessary choice to protect the security of enterprise information assets.

The content of safety training and education includes: (1) Elaborate the basic knowledge of information security, including basic concepts, principles, goals, and other aspects of information security. (2) Emphasize the information security laws and regulations: Introduce the national and local laws and regulations related to information security. Emphasize the importance of complying with laws and regulations to prevent illegal and irregular behavior. (3) Ensure information security risk awareness: Educate employees on how to identify information risks and understand various common information security threats. Enhance employee awareness of information security risks and enhance prevention awareness. (4) Elaborate information security operation specification: Educate employees to master information security operating standards, such as password management, network security usage, software installation, etc. Reduce information leakage and security incidents caused by human factors. (5) Force security technology training: Train a group of information security technology experts to enhance the company's information security protection capabilities. Cover key technical fields such as network security technology and encryption technology.

The methods of safety training and education includes: (1) Offline training: Regularly organize information security training courses and invite experts to give face-to-face lectures. Provide opportunities for centralized learning to ensure training effectiveness. (2) Online training: Utilize online platforms to set up online training courses. Employees can choose to learn according to their own time and needs, which is flexible and convenient. (3) Internal communication and sharing: Organize internal information security experience sharing meeting. (4) Encourage employees to share their practical experiences in information security. (5) Regularly organize drills to simulate information security incidents. Enable employees to learn information security knowledge and coping strategies in real-life situations.

The cycle and frequency of safety training and education includes: (1) New employee onboarding training: New employees must receive comprehensive information security training upon joining. (2) Regular training: It is recommended to conduct information security training for all employees at least once a year. (3) Technical personnel training: Personnel engaged in information security management or technical work should participate in specialized information security management or technical training at least once a year.

The evaluation of effectiveness of safety training and education includes: Evaluate the training effectiveness of employees through exams, questionnaires, and other methods. Adjust and optimize training content and methods in a timely manner based on the evaluation results.

Through comprehensive and systematic security training and education, employees can enhance their awareness and skills in information security, and reduce information security risks caused by human factors, which is of great significance for protecting the security of enterprise information assets.

5 Confidentiality Agreements and Non-Compete Agreements

Confidentiality agreements and non-compete agreements aim to protect sensitive information and commercial interests of the company. The following is a clear explanation of these two agreements.

A confidentiality agreement is an agreement between the parties that one party shall not disclose any written or oral information (i.e. confidential information) to any third party. The agreement should clearly define the scope of confidential information, such as technical information, business information, customer information and the recipients and providers of confidential information, as well as their respective confidentiality responsibilities. The confidentiality period may exceed the duration of the employment relationship and continue for a period of time after the employee resigns. This may include non-compete clauses, payment of confidentiality fees, and return of information to employees upon resignation. If a party with confidentiality obligations violates the agreement, they will bear civil compensation liability. Confidentiality agreements are crucial for protecting a company's trade secrets, technical secrets, business information, etc., and for preventing these information from being leaked to competitors or improperly used.

Non-compete agreement refers to the prohibition by law or employer through labor contracts and confidentiality agreements that employees are allowed to work part-time that competes with their employer during their tenure. Clearly define the prohibited business scope, geographical scope, etc. Non-compete period is generally not exceeding two years, but can be agreed upon based on specific circumstances. In order to ensure the quality of life of workers during the non-compete period, employers should provide monthly economic compensation to workers. If the employee violates the non-compete agreement, they shall pay a penalty to the employer in accordance with the agreement. Non-compete agreements help protect the company's business interests and prevent employees from using their acquired trade secrets, customer relationships, and other resources to harm the company's interests after leaving.

Overall, confidentiality agreements and non-compete agreements are important components of human resource management in information security management. The confidentiality agreement ensures that sensitive information of the company is not disclosed, while the non-compete agreement protects the company's business interests from being harmed by resigned employees. By properly formulating and implementing these agreements, enterprises can effectively manage human resource, maintain their own information security and business interests.

6 Handling of Termination or Change of Appointment

In information security management, the handling of termination or change of appointment in human resource management is a crucial step aimed at ensuring effective protection of organizational information security in the event of employee resignation or change of responsibilities. The following is a clear explanation of the processing flow and the key steps.

Preparation before termination or change of appointment: (1) Information security audit: Before an employee resigns or changes their responsibilities, conduct an information security audit to ensure that the employee has not leaked or taken away sensitive information. (2) Information asset recovery: Recycling company equipment, storage devices, and other information assets used by employees to prevent information leakage.

Handling of termination or change of appointment: (1) Permission recovery: Immediately cancel or modify the system access permissions of departing employees or employees with changed responsibilities, ensuring that they are no longer able to access sensitive information. (2) Key time point: Complete permission recovery on or before the day of employee resignation or change of responsibilities. (3) Password change: Change all passwords and access keys related to resigned employees or employees with changed responsibilities. (4) Security considerations: Ensure the complexity and security of new passwords to avoid guessing or cracking. (5) Data backup and cleaning: Back up important data and clean up personal data and files of former employees or employees with changed responsibilities in the system. (6) Data protection: Ensure the integrity and recoverability of data backups. (7) Notify relevant parties: Notify other employees, partners, and suppliers of changes in the authority of departing employees or employees with changes in responsibilities, to avoid misunderstandings or misuse of information. See Figure 4.

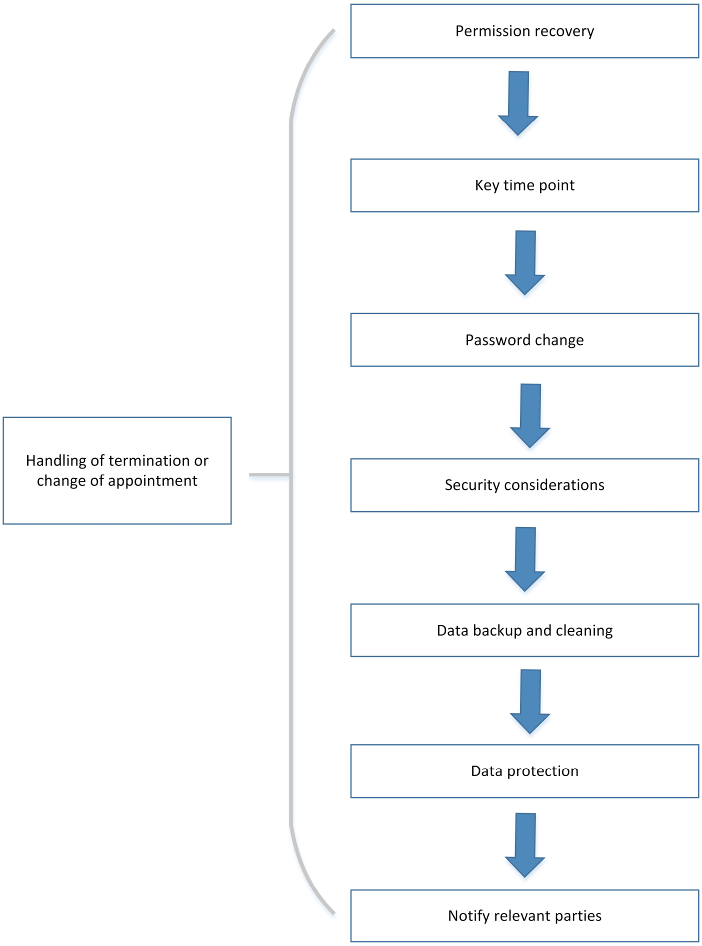

Fig. 4. Seven steps of handling of termination or change of appointment.

Follow up after termination or change of appointment: (1) Supervision and inspection: During a period of time after an employee resigns or changes in responsibilities, supervision and inspection are carried out to ensure that all relevant processes and measures are implemented. (2) Record and document: Record the entire processing process, including recovered assets, changed permissions, and passwords, for future reference or auditing. (3) Update responsibility allocation: Based on employee turnover or changes in responsibilities, update the organization's responsibility allocation matrix and personnel allocation management plan.

Key precautions: (1) Timeliness: Ensure that all necessary processing steps are completed on or before the day of employee resignation or change of responsibilities to reduce the risk of information leakage. (2) Confidentiality: Ensure that all information and data involved are properly stored throughout the entire processing process to avoid leakage to unauthorized personnel. (3) Compliance: Ensure that all processing steps and measures comply with relevant laws, regulations, and organizational policies to avoid legal disputes or compliance risks.

By implementing the above steps and precautions, it can be ensured that the termination or change of human resource management appointments in information security management can be effectively executed, thereby protecting the organization's information security [9, 10, 11].

7 Conclusion

Human resource management is at the core of information security. It not only involves the protection of internal information within the organization, but also relates to the overall operation and reputation of the organization. Personnel are the core of information security management. Training and education helps to improve the overall security level of the organization, and also reduces the probability of information security incidents. When employees resign or transfer position, we must ensure that they no longer have access to sensitive information and clear their relevant data and records. Human resource management requires the participation and collaboration of many departments and all staff, who jointly develop and implement security strategies and measures. In one word, human resource management in information security management is a complex and important task. Only through comprehensive, systematic, and effective management of human resources can we ensure that an organization's information assets are fully protected.

Acknowledgments

This work was supported by Research Funds for NSD Construction, University of International Relations, grant No. 2024GA06.

References

1. Michael E. Whitman, Herbert J. Mattord. 2017. Principles of Information Security, Cengage Learning, 6th edition.
2. Pawel Kobis. 2023. Classification of key human factors in the area of information resources security management in small enterprises in Poland. KES 2023, pp. 1641-1650.
3. Kamphol Wipawayangkool. 2010. Strategic Role of Human Resource Management in Information Security Management. AMCIS 2010, vol. 20, pp. 1-6.
4. Kamel Mohammad Al-hawajreh, Muhammad Bajes Al-Majali, Menahi Mosallam Alqahtani, Basem Yousef Ahmad Barqawi, Sulieman Ibraheem Shelash Al-Hawary, Enas Ahmad Alshuqairat, Ayat Mohammad, Muhammad Turki Alshurideh, Anber Abraheem Shlash Mohammad. 2023. Develop a Causal Model for the Impact of Critical Success Factors of the Strategic Information System in Promoting Human Resources Management Strategies in the Social Security Corporation. The Effect of Information Technology on Business and Marketing Intelligence Systems 2023. pp. 903-921.
5. Dorothea Kossyva, Georgios N. Theriou, Vassilis Aggelidis, Lazaros Sarigiannidis. 2024. Retaining talent in knowledge-intensive services: enhancing employee engagement through human resource, knowledge and change management. J. Knowl. Manag. 28(2), pp. 409-439.
6. Richard Johnson, Kristine Kuhn. 2024. Information Technology and Human Resource Management: Revisiting the Past to Inform the Future. HICSS 2024, pp. 6300-6309.
7. Juan Manuel Maqueira-Marín, Diéssica Oliveira-Dias, Nima Jafari Navimipour, Bhaskar B. Gardas, Mehmet Unal. 2022. Cloud computing and human resource management: systematic literature review and future research agenda. Kybernetes 51(6), pp. 2172-2191.
8. Yanhua Yang, Yu Wang. 2022. Enterprise Human Resources Recruitment Management Model in the Era of Mobile Internet. Mob. Inf. Syst. 2022, vol. 7607864, pp. 1-6.
9. Heli Ikonen, Virpi Jylhä, Hanna Kuusisto. 2022. Lack of Human Resources Leads to Breaches in Information Management Processes. MIE 2022, pp. 159-163.
10. Wenjia Xie, Shaofeng Lin, Changfu Dong, Wanli Kou, Meimei He. 2021. Security Management for Human Resource Data Based on Blockchain Technology. DSDE 2021, pp. 12-16.
11. Youngkeun Choi. 2017. Human Resource Management and Security Policy Compliance. Int. J. Hum. Cap. Inf. Technol. Prof. 8(3), pp. 68-81.