iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42978

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Human Resource Security in IT Sector

P. Pooja[1], B. Greeshma[2]
[1]*B.com student, VITBS, Chennai*
[2]*HR Executive, HCL Technologies, Chennai*

Abstract: ***In any organization specifically in any IT industry — security is a major issue and it relates to the Human Resource Department. In this paper, we summarize the importance of security and focus on the responsibilities of the HR Department. The responsibilities vary and depending on what method the organization wants to follow, starting from the date of entry of an employee to the last date of working with the employee. This article concludes by providing the methods for data protection using Human Resource Security and how it helps the HR Department to control the rate of employee attrition by increasing the rate of employee retention in an organization. In this process, the HR Department would' be making the employees understand the importance of data protection until the last date of their work in the organization using Human Resource Security.***
Keywords: Human Resource Security, Information Securities, IT Sector, employees.

I. INTRODUCTION

Human Resource Security in any organization especially in an IT Sector is the process that starts before, during, and after the employee's date of joining and ends at when the employee exits from the organization. The main objective of Human Resource Security to educate all the employees of an organization about their procedures and policies of Information security and make them understand duties and responsibilities that are suitable to their job roles and this access will be completely blocked, once the period of employment of the employee is terminated or relieved (in the normal course or other cases), from their system.

When it comes to human resource security it applies to all industries but in this article, we focus on how important is human resource security in the IT Sector and what are major issues that an HR department faces when it comes to information security, and how it helps control the rate of employee attrition by increasing the rate of employee retention in an organization.

II. PRIOR TO EMPLOYMENT PROCESS

When it comes to the human resource securities, these are the important aspects of Information security. The HR should ensure that the employees and contractors do understand their responsibility in identifying candidates suitable for the job role as per the requirement. The process Prior to Employment, mainly focus on the following two aspects:

A. Screening

The first and foremost process of the HR department when it comes to human resource security is screening. Screening, usually before HR induction, starts from the process of background verification and competence check on all applicants for employment. The background verification and competence check process should be carried out based on the business requirement as per their governing laws, regulations, and ethics keeping in mind the risk associated with access provided for the data information. The screening is not only restricted for company employees it is also applicable for the contractual employees. A sufficient number of documents required are collected and shared during the document verification. HR audits - which deals with these data is expected to see that distinct procedure is steadily carried out at every time without any hindrance and avoid proclivity to any employee which will become the process of overall organization hiring process. Once the background verification and competence check are successfully over, the offer for the applicant will be provided.

B. Terms and Conditions of the Employees

The next important process of human resource security is to carry out the terms and conditions of an employee. The HR department needs to provide adequate knowledge about the employee's terms and conditions to the applicant during the process of HR Induction. The contractual agreement must contain what the organization's responsibilities are and that employees and contractors need to stick to it when it comes to information securities. This is the right time to educate the employees about information security in general and individual responsibilities since it is very important as regards GDPR and the Data Protection Act 2018. The agreement should have the reference and contain an overall range of control areas that has to include IPR ownership, return of assets, and overall compliance with the ISMS as well as more specifically acceptable use, etc.

The employee should be aware, before giving an acknowledgment, that if they breach any of these terms and conditions mentioned in the agreement after they join the organization then they will face legal consequences.

III. PROCESS DURING EMPLOYMENT :

In this process, HR needs to ensure whether the employees and contractors are aware and satisfy their information security responsibilities during the period of employment since they have the access to the sensitive data. This process mainly focuses on three aspects that are:

1) Management responsibilities
2) Information Security Awareness, Education & Training
3) Disciplinary Process

A. *Human Resource Responsibilities*

The quality control will educate the organizational employees and contractual employees on how to use information securities according to the organization's policies and procedures. It is the responsibility of the organization's HR to ensure that their employees are aware of the information security threats, controls, and vulnerabilities related to their job by providing adequate training according to the information Securities policy and control; the requirements of the terms, and conditions of employment. The organization's HR needs to ensure security awareness and uprightness in developing the appropriate security culture for the entire organization.

B. *Information Security Awareness, Education & Training*

HR needs to ensure that either its organizational employee or contractual employee should receive adequate education and training to fulfill their job requirements securely. They need to be provided with frequent updates as per the changes that occur in the organization's policies and procedures and also make them understand the applicable legislation that affects their roles. The HR department needs to organize a Learning & Development session by partnering with the information security team to accomplish the skills, knowledge, competence, and awareness assessments and to plan and implement a program of awareness, education, and training throughout their employment period. Not only the employees even the auditors need to be provided with the demonstration of adequate training and compliance, as this will also help the audit team to have a better understanding of how the staff and contractual employees are educated concerning training and awareness.

C. *Disciplinary Process*

The disciplinary process needs to be communicated and documented to all the employees and contractors to keep the process in place. Disciplinary action will be taken against the employee if there are any security breaches. This process should begin after prior verification that an information security breach has occurred. When an employee is suspected of an information security breach he or she should be treated without any partiality. The disciplinary process is implemented to prevent the employees from violating the organization's information security policies and procedures. So, we should consider some factors before deciding the action, such as the nature of the breach and its impact on the business requirements, has employee done the security breaches repeatedly or for the first time, has the suspect got the proper training concerning the violation, relevant legislation, business contracts, and other factors as required. Immediate action should be taken in case of deliberate breaches.

D. *Termination or Change of Employment Responsibilities*

The Information security rules and regulations will be valid even after the employee's termination or change of employment. It should be communicated and defined to employees and contractors and enforced. The organization and all employees will have a confidential agreement that contains the appropriate ongoing information security requirements and legal responsibilities. The terms and conditions will continue even after the end of employment for the defined period as per the confidential agreement in that they have some clear responsibility that remains even though the employee has moved away from the organization. It's not just at the time when the employee exits or terminates, it's even applicable, for change of employment, role access not related to their new job role will be removed and will be provided only for information assets needed for the new job role. All the access will be blocked once the employment of the employee is terminated or relieved from their system. An employee will receive the experience letter from the organization only after he/she has surrendered all the organizational-related assets and documents because these need to be closed officially by documenting in the asset inventory. The HR department needs to inform the auditor that the employee has surrendered their asset after the exit or termination as per the documentation in the asset inventory.

IV. WHY HUMAN RESOURCE SECURITY IS IMPORTANT IN IT SECTOR:

The IT Industries deal with many confidential and delicate data related to their business demand. The data is used in many developments, services, and marketing, etc. and these data are at higher risk of being hacked if there are no proper security measures in information security. When an employee is hired, the IT sector will initiate background verification based on certain factors, for example, any criminal record in the past or previous employment and even need to check their health based on their business requirements, etc. An IT employee joins the business as per his job role, need to understand terms and conditions related to information securities and violation. HR needs to convey and make the employee understand all the terms and conditions before the acknowledgment. The Human Resource department in the IT sector needs to carry out adequate training to the employees frequently about data protection policy and Information securities threats, controls, and vulnerabilities related to their job. The Human Resource security in the IT sector will have to change and update as per the business requirement. The disciplinary policy will be strictly followed since they should be very careful because security breaches can happen at any cause. When an employee exits from the IT industry, from the same day the candidate will have no access to any of this information. The HR department should conduct frequent Training and development induction for the employees to help them to brush up on existing rules and get educated if there any new updates.

A. Ways to Increase Employee Retention

1) Explain the job roles and responsibilities clearly while hiring the employee.

2) Make the employees understand why the BGV competence check is required. The employee should feel free to share all the required data. He or She should not think the organization is entering into their personal information.

3) Give the employee the chance to understand the terms and conditions for the organization and job role. During induction or orientation allow the employee to have the doubts cleared before providing their acknowledgment.

4) The employee is not in general allowed to get involved in management or training. Check with the employee to find out what issues he/she is facing in this job or organization.

5) Even after providing adequate education and training if an employee is unable to fulfill their job requirements securely, get into a conversation with an employee and understand where he/she is lacking and provide the necessary training.

6) The disciplinary process needs to be communicated and documented to all the employees. If a security breach has happened and the employee connected with has done it by mistake (not deliberately) educate the employee once again.

7) A satisfied employee with all the understanding and knowledge about the process and organization should be encouraged to work towards organizational goals fulfilling all the requirements securely.

8) The rate of attrition will increase only when there are unhappy employees in the organization and when candidates do not understand or are not trained and unable to fulfill the business requirement.

9) By educating all the employees and make them understand the job roles and responsibilities using Human Resource security as suggested by the above measures, the employees will feel free to approach the HR department. This approach and understanding of the work environment are very likely to increase the rate of employee retention.

V. CONCLUSION

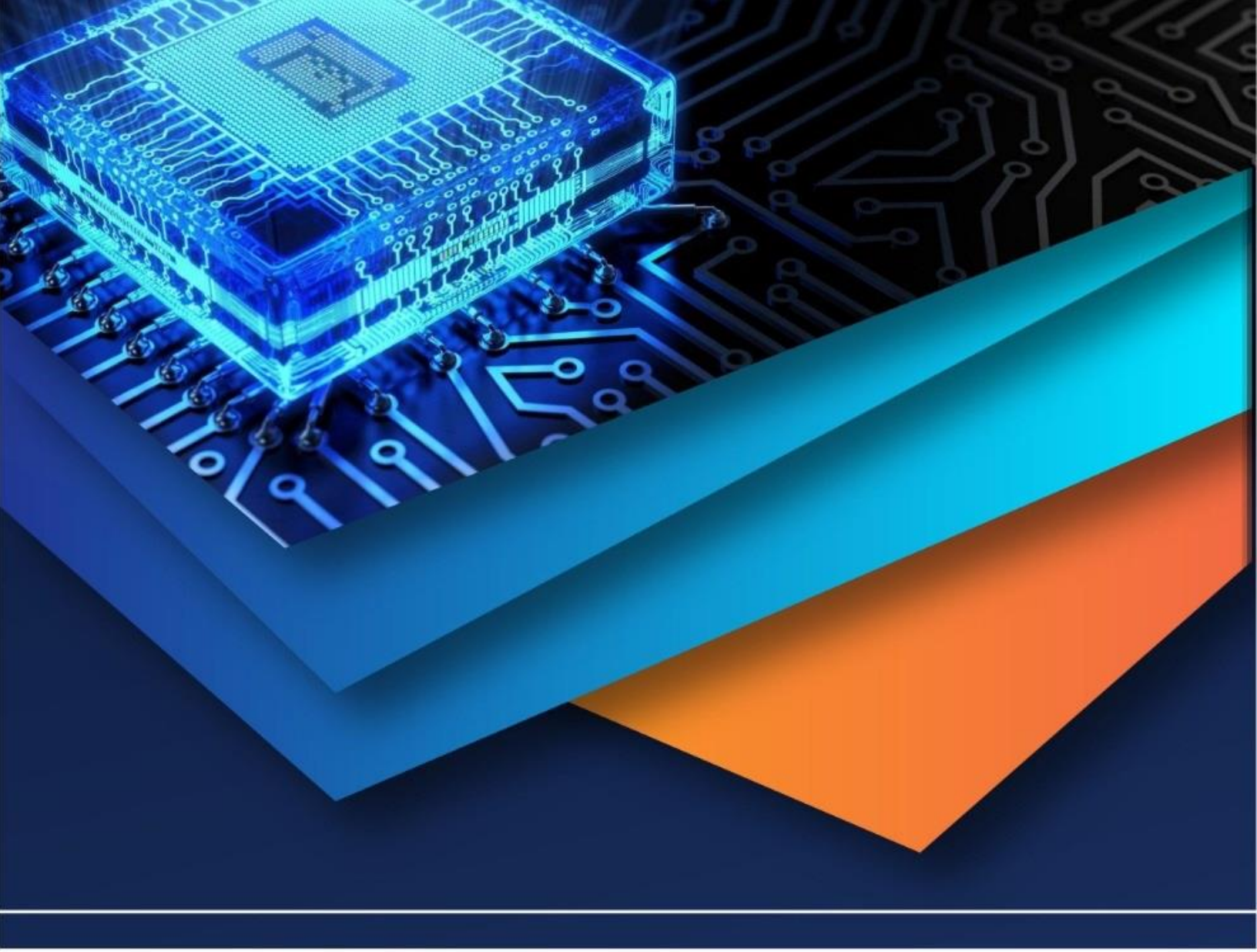
This paper is based on the Importance of Human Resource Security in an Organization. The main purpose of this paper is to understand why Human Resource security is used in an organization related to IT Sector and what is the process that the HR department needs to follow when it comes to Human Resource security. This study has explained how the Human Resource security process happens before, during, and after the employee's date of joining and ends when an employee exits from the organization. This paper Mainly focuses on four factors Human Resource Security, Information Securities, IT Sector, Employees. It has even covered why Human Resource security is important when it comes to the IT sector and what are ways to increase rate employee retention. Thus the paper concludes that the rate of employee retention can be increased by using Human Resource security by making the employees understand the process of Information security according to the job requirement and organization policies.

REFERENCES

[1] Barkha Gupta (2013). Human Resource Information System (HRIS): Important Element of Current Scenario,IOSR Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 13, Issue 6 (Sep. - Oct. 2013), PP 41-46.

[2] Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16, 377–397.

[3] Humayun Zafar (2013).Human resource information systems: Information security concerns for organizations.Human Resource Management Review, Volume 23, Issue 1, March 2013, Pages 105-113.
[4] Lewis, R. (2014). What HR can do prevent data breaches and cyber threats. [Online]. http://www.humanresourcesonline.net/hr-can-help-prevent-data-breaches-cyber-threats/ Accessed 11th January, 2018.
[5] Nik Nordiana Binti N Ab Rahman, Setyawan Widyarto (2013). Information Security: Human Resources Management and Information Security Incident Management, ICIBA2013, the Second International Conference on Information Technology and Business Application Palembang, Indonesia, 22-23.
[6] Subramaniyan, S., Thite, M. & Sampathkumar, S. (2019) Information security & privacy in eHRM. In M. Thite (Ed.). e-HRM: Digital Approaches, Directions & Applications, Abingdon, UK: Routledge. P. 250-267.
[7] Stine, K., Kissel, R., Barker, W. C., Lee, A., & Fahlsing, J. (2008). Volume II: Appendices to guide for mapping types of information and information systems to security categories. Available at. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf. Retrieved May 25 2011.
[8] Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17, 4–19.
[9] Wipawayangkool, K. (2010). Strategic role of human resource management in information security management. Paper presented at the 16th annual Americas Conference on Information Systems, Lima, Peru, 12–15.
[10] Youngkeun Choi (2017). Human Resource Management and Security Policy Compliance. International Journal of Human Capital and Information Technology Professionals (IJHCITP) 8(3), 3-14.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY