Information Security Management System

Software Copyright, License & Compliance Policy & Procedure

Document no. JMBGRP/ISMS/Pol-SC

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The purpose of this policy is to ensure that JMBGRP abides by the Software Copyright and license laws and regulations.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT Dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to “References”	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Modifications done in Section: “Scope, Procedure”	

Contents

Purpose

The purpose of this policy is to ensure that JMBGRP abides by the Software Copyright and license laws and regulations.

Scope

This policy applies to all employees;(Business owners, custodians, system administrators, software developers and users) of information who are authorized to use internet facilities provided by the company.

Policy Statement

- The procurement of software licenses at JMBGRP shall be through a formal process and shall be justified through business case only.
- The licenses which are procured are for end users, for network Infrastructure devices and applications which have pan company deployment such as ERP Platform (SAP), CRM Platform, Windows (Desktops /laptops) / Apple IOS for end user computing, UNIX Licenses , Windows Licenses for Servers , IOS for Routers and Switches, Applications for mobile users. JMBGRP also procures specific licenses for businesses as per the need.
- JMBGRP shall ensure that all the necessary measures are instituted to ensure that software copyright compliance is always maintained.
- Needless to say compliance to software copyright compliance is not only the responsibility of IT which is the principal distributing and management agency, but also that of individual employees and departments.
- JMBGRP shall be committed to ensure that their employees' comply with existing copyright law of country and various software licenses where JMBGRP has been a signatory. Further JMBGRP shall thrive to attain the following :
    - Encourage the lawful use of copyright protected software applications.
    - Respecting ownership rights of intellectual property vested with software.
    - Provide guidance and mechanisms to enable stakeholders to meet their legal obligations.
    - Prevent and rectify unlawful use of copyright material.
- Installation and Usage of Freeware, shareware and open-source software applications are strictly prohibited and shall be permitted through the exception process only.
- Adequate care shall be taken to ensure that installations of any software shall not cause any disruption or damage to the existing applications / operating systems or databases.
- Installable software code and media duplication, transmission through JMBGRP's network or to the outside world shall be permitted through necessary approvals only.
- Review of Licenses will be done by IT and new licenses shall be procured based on business need.
- IT shall have the right to audit end user machines to check for the software's and licenses installed. For the same there shall be a tool based compliance approach adopted.

- JMBGRP information technology infrastructure and applications shall only have licensed software deployed on them.
- Any software copyright violation by employees shall lead to a disciplinary action and may escalate to a legal action as the case may be.

Procedure

1.1. The procedure on Software License Management shall cover the following areas

1.1.1. Software Procurement

1.1.2. Software Maintenance

1.1.3. Evaluation

1.1.4. Distribution

1.1.5. Deployment

1.1.6. Transfer

1.1.7. Return

1.1.8. Software Use

1.1.9. Violation & Incident Reporting

1.1.10. Responsibility

1.2. **Software procurement**

1.2.1. IT shall manage centralized procurement or sourcing of software applications as a single window based on the business requirement and distribute them to the respective businesses and locations as per requirement.

1.2.2. **Procurement**

1.2.2.1. Procurement team shall procure the licenses as per the requirement posted by IT. Once the licenses are delivered to IT. The identified IT Team shall maintain the following records in the software license register.

1.2.2.1.1. Name of software.

1.2.2.1.2. Number of licenses.

1.2.2.1.3. Date on which the license come into force (if applicable).

1.2.2.1.4. Number of licenses utilized.

1.2.2.1.5. Date on which the license expires (if applicable).

1.2.2.1.6. Nature and description of licenses.

1.2.3. Post the receipt of the E-licenses, necessary back-up copies shall be made as per the licensing agreement and media along with the license documents shall be stored in a fire proof cabinet. The license keys shall also be placed in the fire proof cabinet.

1.2.4. Existing Software application details are maintained separately.

1.2.5. For any software's, which are not a part of the table, the necessary requisition has to be made by departments to IT which shall facilitate the procurement through the procurement team.

1.2.6. Employees shall not buy any software on their own accord and install or attempt to install it on their systems.

1.2.7. IT shall review the license requirement every year and shall decide upon the numbers to be procured afresh, which licenses not to procure at all.

1.2.8. **Maintenance**

1.2.8.1. The license management team at IT shall be responsible for maintaining the procured licenses. The team shall ensure that unauthorized copies are not made, license keys are not shared, unauthorized installations are not done and there is no fraudulent activity related to reselling or distribution of the procured licenses.

1.2.8.2. The software license maintenance team in IT Team shall be responsible for doing an audit at least on an yearly basis to check for:

1.2.8.2.1. Procured Licenses

1.2.8.2.2. Installed Licenses

1.2.8.2.3. Expired Licenses

1.2.8.2.4. Licenses available

1.2.8.2.5. Unauthorized software's

1.2.8.2.6. Employee / Dept. to whom the software license has been issued

1.2.8.2.7. Date of issue

1.2.8.2.8. Record of acknowledgement of receipt

1.2.8.2.9. Date of return

1.2.9. A tool based approach shall be deployed to perform this audit and also initiate remediation to remove all unauthorized software's on end user systems and those which might be installed on servers as well.

1.2.10. Employees & IT shall be responsible for reading, understanding and adhering to all applicable licenses norms , notices, contracts and agreements as will be applicable for software that is to be used on company machines. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation law relating to copyrights. In addition to violating such laws, unauthorized duplication of software is a violation of company's Software Policy

1.2.11. Employees and third parties who are doubtful about the permitted usage of a licensed software application or JMBGRP developed software application shall contact IT for explanations and clarifications. Also it is a primary duty of IT to communicate the permitted usage of licensed and developed software application(s) with a periodicity of 12 month's upon acquirement and for renewal as the case may be.

1.2.12. JMBGRP's licensed software application and developed software applications provided to employees of various category and third parties shall abide the terms of the relevant license agreement. Such terms shall be inclusive of the following but not exhaustive:

1.2.12.1. Making multiple copies of a product for personal or other persons' use

1.2.12.2. Copying the source code/logic of application developed by JMBGRP

1.2.12.3. Cracking/jail-breaking and Uploading the product acquired or developed in whole or in part in a website or blogs.

1.2.13. **Evaluation**

1.2.13.1. For every license which has been purchased, the same shall be deployed on the test systems; this includes standard licenses.

1.2.13.2. The reason of above is that new release of any software has certain enhancements and these enhancements shall not in any way impact the already functioning systems and applications.

1.2.13.3. Hence all server upgrades, network device iOS upgrades and patches, oracle patches, Microsoft Service Packs and patches shall first be tested and then be deployed.

1.2.13.4. For a major version change adequate testing shall be done before deployment.

1.2.13.5. When an employee has requested for a business specific tool or software, the same shall also undergo testing before it is released.

1.2.13.6. The concerned IT team shall endeavor to find similar products and compare them and also undertake to conduct a POC before deciding upon what to purchase.

1.2.13.7. Testing shall be done to ensure that user systems don't get impacted in case of freeware also..

1.2.13.8. Every software deployed on JMBGRP systems shall be tested and certified by IT for it-team safety.

1.2.14. **Distribution:**

1.2.14.1. Distribution of licensed software shall be carried out only by the Software Team at IT and shall conform to software licensing agreements. In particular, the number of copies of software distributed shall not exceed the number of licenses entitled for use. A copy of licensed software shall be deemed to be issued after it is installed on a computer. Alternatively a dedicated portal shall hold repository of all licensed products which shall be allowed to be installed by authorized personnel only.

1.2.15. **Deployment**

1.2.15.1. Any user who needs a copy any additional software's shall get the necessary approvals from the HoD, who in turn shall forward the request to the IT License Management Team.

1.2.15.2. There has to be written justification with a business for requisition of specific licenses of software's

1.2.15.3. Once the E-license is procured, the IT person shall install the license on the identified systems and then store the media and the keys in the fire proof cabinet in IT Department.

1.2.15.4. Post installation of the newly procured non-standard software, the IT person shall update the software Inventory.

1.2.15.5. For end user systems which require re-install of the operating system or the Office Components, the same shall happen through a request to IT.

1.2.15.6. The IT person shall come with the appropriate media, make the installation and leave.

1.2.15.7. The media and the key shall not be provided to the employee, they shall always remain in the custody of IT.

1.2.15.8. Terms and conditions of the software licensing agreement shall be communicated to users to whom the software is issued. This communication can happen either in periodic information security training or specialized trainings or during the time of installation.

1.2.15.9. During the installation IT person shall not install any installation code copies or software images on the user system, which could be later misused.

1.2.16. **Transfer:**

1.2.16.1. An owner (user/ department) of a copy of licensed software shall not directly transfer his/her ownership to any other user.

1.2.16.2. Only IT can initiate transfer of licenses if there is a provision of transfer in the original licensing agreement.

1.2.16.3. The IT person shall ensure that the software on the system(s) is uninstalled from the identified hosts and then update the software license registry.

1.2.16.4. The transfer agreement if it is not a part of the original license agreement shall be kept together with the original license documents by IT.

1.2.17. **Return**

1.2.17.1. The return of license can happen in seven scenarios:

1.2.18.1.1. Resignation of an employee

1.2.18.1.2. Transfer of an employee

1.2.18.1.3. Termination of an employee

1.2.18.1.4. Loss of machine/Malfunction – desktops/laptops/smart phones / tablets

1.2.18.1.5. Decommissioning of Infrastructure Devices (servers, routers, switches)

1.2.18.1.6. Decommissioning of any existing application

1.2.18.1.7. Upgrade of existing application with a new version from the one installed currently.

1.2.17.2. A copy of licensed software shall be deemed to be returned after it is uninstalled from a computer by the personnel from IT and the register updated.

1.2.17.3. The IT team shall proactively create renewal plans for the licences which are near expiry keeping in view the lead time for getting approvals from the various levels.

1.2.17.4. After renewal, IT team shall update the software inventory register.

1.2.17.5. Ownership shall cease on expiry of the software license.

1.2.18. **Software use**

1.2.18.1. A user to whom a copy of software is issued shall abide by the terms and conditions of use that are communicated to them by the IT team.

1.2.18.2. Users are prohibited from making unauthorized copies of shrink-wrapped software installed on JMBGRP computers. Backup copy of the software media shall comply with licensing agreement of the software.

1.2.18.3. Notwithstanding anything contained in the software licensing agreement all users of software shall comply with applicable Intellectual Property laws e.g. The Copyright Act, 1957, and Information Technology Act, 2000. As amended 2008 The users shall not make unauthorized copies of the software.

1.2.18.4. The users shall request for software which is required only for business purpose.

1.2.18.5. The users shall not get software installers on external media.

1.2.18.6. The users shall not try to install any shareware/ freeware on their own.

1.2.18.7. The users shall not try to install patches/ updates on their own.

1.2.18.8. Mobile users (tablets, smart phones) – shall only install software's which are approved by the IT.\

1.2.18.9. Infrastructure Team will install software with planned downtimes and taking utmost care in the configuration post installation to ensure that the servers / devices get back to business-as-usual status. Appropriate ticket shall be generated for new installation using Ticketing Tool. The same process shall be applied while applying application patches to the existing functional applications at JMBGRP. Application upgrade process shall be the same for the applications developed in-house.

1.2.18.10. During reinstallation / service pack upgrades / version upgrades, if the IT person recommends a backup of the system to be taken then the same shall be done through the IT Help Desk.

1.2.18.11. For infrastructure devices as well, a configuration back up shall be taken along with rule sets to ensure that normalcy is restored if the installation could not achieve it-team objective..

1.2.18.12. License upgrades / version upgrades to servers shall be done in a test environment and the servers and then shall be released into production.

1.2.19. **Violations and incident reporting:**

1.2.19.1. Any breach/violation by an unauthorized use such as copying, cracking, replicating or duplicating the source code/logic of JMBGRP's acquired software applications or JMBGRP's developed software applications or other software licensed works is prohibited and is subject to disciplinary action as laid down in JMBGRP's code of conduct.

1.2.19.2. In general, reporting any violations to this policy shall be directed by department head/chief to IT.

1.2.19.3. At Locations - by sending e-mail to administrators or calling respective numbers.

1.2.19.4. If possible, please forward a copy of any information relevant to the incident you are reporting.

1.2.19.5. If it isn't clear where to report the problem, you may send it to IT Helpdesk who shall redirect the incident to the appropriate person(s) for action or shall handle it directly. (is there no Incident id has been finalized)

Responsibilities

The responsibility for the planned initiative in this document lies with the following personnel:

- Head of Department:
  - Approve/Authorize user request for a copy of licensed software.
  - Approve / Authorize user request for any special software as required by business.
  - Facilitate in the license audit with IT
  - Cooperate with HR where disciplinary action is required to be taken.
- HR:
  - Executing disciplinary action
- IT License Management Team :
  - Maintain custody of software licenses.
  - Maintain software licenses inventory.
  - Approve user's request for licensed software.
  - Approve procurement of new software license.
  - Ensure that the transfer of ownership of software is in accordance to the licensing agreement.
  - Maintain the transfer agreement.
  - Ensure maintenance of software asset register.
  - Maintain software media, license keys and other evidence of ownership throughout it-team lifecycle in a fireproof cabinet.
  - Ensure maintenance of backup copies of licensed software Report security incidents relating to software copyright to IT Security Team and Head GIS.
  - Ensure conduction of annual audit software inventory.
  - Review the user request for software initiate procurement.
  - Track license expiry and initiate renewal process.

- Testing of software before deployment (licensed software and free ware and shareware)

- IT Help Desk :
  - Installation and uninstallation of software on user machines.
  - Deletion of unauthorized software's from user machines
  - Provide report to the Head - License Management Team on monthly activities conducted.
  - Highlight violation, misuse to HOD
- Users:
  - Submit a request for software requirement.
  - Adhere to terms and conditions of software licensing agreement.
  - Log calls with IT Helpdesk to report any problems with the installed software's.
  - Comply with applicable Intellectual Property laws e.g. The Copyright Act, 1957 and Information Technology Act, 2000 as Amended by act of 2008.

Enforcement:

- This policy and procedure is applicable for all the employees of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct.
- Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this document at any time as per it-team discretion.

Metrics

- The metrics shall be reported to the Head GIS and then to Security In-Charge on a quarterly basis by the IT License Management Team.
- The metrics to be reported , but not restricted to include:
  - Number of software licenses procured and not deployed.
  - Number of licenses expired.
  - Number of licenses which have not been renewed.
  - Number of users to number of actual licenses available
  - Multiple software's for similar or same type of job
  - Number of users who have been provisioned/enabled with that as service or installed in their machine.
  - Number of breaches/violations by stakeholders, upon which disciplinary proceedings invoked.
  - Audits findings about installed versus permitted application.

Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.
- Exceptions to this Security Policy and Procedures shall be allowed at the time of implementation of this policy and procedures or at the time of making any updation to this

document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which shall be of temporary or permanent in nature.

- All exception requests shall be submitted by respective HODs/Security In-charge. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.
- The Security In-Charge shall review all exceptions, as the case may be, every year for validity and continuity.

Disclaimer

- JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Acceptable usage Policy and Procedures document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the Apex Committee. The Acceptable usage policy and procedure document is meant to be published on the intranet of JMBGRP and/or any other forum as decided by the management of JMBGRP. Anything not specifically stated in this Acceptable usage policy and procedure document shall not be considered as implied in any manner.
- For any clarifications related to this Acceptable usage policy and procedure document with respect to it-team interpretation, applicability and implementation, please raise a request in Ticketing Tool.

References:

- Control Objectives: A.5.19, A.5.20, A.5.21