JINDAL SAW LTD.
TOTAL PIPE SOLUTIONS

JINDAL SAW LIMITED

IT POLICY – V1.2

(USER LEVEL GUIDELINES)

Approved by: Date: 29.4.2024
Mr. Chandan Sinha
(Group CIO)

INDEX

Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at Jindal SAW. These rules are in place to protect the employee and Jindal SAW. Inappropriate use exposes Jindal SAW to risks including virus attacks, compromise of network systems and services, and legal issues.

Building a good security policy and implementing it provides the foundations for the successful implementation of security related projects in the future, this is without a doubt the first measure that must be taken to reduce the risk of unacceptable use of any of the Jindal SAW's information resources.

The first step towards enhancing Jindal SAW's security is the introduction of a precise yet. enforceable security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities.

The development (and the proper implementation) of a security policy is highly beneficial as it. will not only turn all of your staff into participants in Jindal SAW's effort to secure its communications but also help reduce the risk of a potential security breach through "human-factor" mistakes. These are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities.

Additionally, the building process of a security policy will also help to define a Jindal SAW's critical assets and the ways they must be protected and will also serve as a centralized document, as far as protecting Information Security Assets are concerned.

Scope:

This policy applies to employees, contractors, consultants, temporary workers, and other workers at Jindal SAW, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Jindal SAW.

This policy is by no means intended to be a complete reference on the process of building a security policy or the development of a security awareness course. Instead, it was created with the idea of providing the reader with a reliable source of advice, various recommendations and useful tips gathered from my personal experiences while building and developing security policies. This document will also provide you with sample security best practices concerning various information security threats, as well as discuss in detail some of the most common security problems which companies are facing every day.

IT SECURITY POLICY

The security policy is basically a plan, outlining what the company's critical assets are, and how they must (and can) be protected. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information and IT Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the company's critical systems.

The document acts as a "must read" source of information for everyone to use in any way. systems and resources defined as potential targets. A good and well-developed security policy should address some of these following elements:

- How sensitive information must be handled.
- How to properly maintain your ID(s) and password(s), as well as any other accounting data
- How to respond to a potential security incident, intrusion attempt, etc.
- How to use workstations and Internet connectivity in a secure manner
- How to properly use the corporate e-mail system.

Basically, the main reasons behind the creation of a security policy are to set a company's information security foundations, to explain to staff how they are responsible for the protection of the information resources and highlight the importance of having secured communications while doing business online.

1. ACCESS CONTROL POLICY

1.1 Minimum Password Length:

The length of passwords must always be checked automatically at the time that users construct or select them. All passwords must have at least Six (6) characters

1.2 Choice of Passwords - Difficult-to-guess Passwords required:

All user-chosen passwords for computers and networks must be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" must not be employed. Likewise, personal details such as own/ spouse's/children name, automobile license No, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed.

1.3 Storage of Passwords:

Employees must maintain exclusive control of their personal passwords; they must not share them with others. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access controls, or in other locations where unauthorized persons might discover them.

1.4 Cyclical Passwords Prohibited:

Users are prohibited from constructing fixed passwords by combining a set of characters that do not change with a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project, or some other easily guessed factor. For example, users must not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.

1.5 User-chosen Passwords must not be reused:

Users must not construct passwords which are identical or substantially like passwords that they had previously employed, they cannot use the last 3 passwords.

1.6 Passwords must contain both Alphabetic and Non-Alphabetic Characters:

All user-chosen passwords must contain at least one alphabetic and one non-alphabetic character. Non- alphabetic characters include numbers (0-9) and punctuation. The use of control characters and other non- printing characters is discouraged because they may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.

1.7 Passwords must contain both Upper- and Lower-Case Characters:

All user-chosen passwords must contain at least one lower case and one upper case alphabetic character. This will help make passwords difficult-to-guess by unauthorized parties such as hackers and industrial spies.

1.8 Pronounceable System-Generated Passwords:

So that users can more easily remember them, and so that users will not need to write them down, all system-generated passwords for end-users must be pronounceable.

1.9 Passwords never in Readable Form when outside Workstations:

Fixed passwords must never be in readable form outside a personal computer or workstation.

1.10 Requirement for different Passwords on different Systems:

To prevent the compromise of multiple systems, computer users must employ different passwords on each of the systems to which they have been granted access.

1.11 Passwords must never be written down near Related Access Devices:

Users must never write down or otherwise record a readable password and store it near the access device to which it pertains. For example, a personal identification number (PIN) must never be written down on an automated teller machine (ATM) card.

1.12 Email Password Policy

Emails users will change their password before 180 days.

1.13 SAP Password Policy

SAP password policy is not changing regularly because of business requirements.

1.14 Users responsible for all Activities involving Personal User-IDs:

Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like "guest").

1.15 End-User Passwords Guidelines

Users can choose easily remembered passwords that are at the same time difficult for unauthorized parties to guess, an example are mentioned below.
If they string several words together (the resulting passwords are also known as "passphrases"),
Shift a word up, down, left or right one row on the keyboard,
Bump characters in a word a certain number of letters up or down the alphabet,
Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word,
Combine punctuation or numbers with a regular word,

Create acronyms from words in a song, a poem, or another known sequence of words,
deliberately misspell a word (but not a common misspelling), or
Combine a few personal facts like birth dates and favourite colours.

1.16 Automatic Log-Off Process:

If there has been no activity on a computer terminal, workstation, or computer (PC) for ten (10) minutes, the system must automatically lock. Re-establishment of the session must take place only after the user has provided the proper password.

1.17 Leaving Sensitive Systems without Logging-Off:

If the computer system to which they are connected contains sensitive or valuable information, users must not leave their computer (PC), workstation, or terminal unattended without first logging-out.

1.18 Logging-Off Personal Computers connected to Networks:

If personal computers (PCs) are connected to a network, when unattended they must always be logged-off.

2. USE OF SYSTEMS

2.1 Games, Personal Videos and Photos may not be stored or used on Official Asset.

The objective of this policy is to clearly state that games, Personal video and Photos must not be used on Jindal SAW Limited system. Games are often downloaded from bulletin boards and may accordingly be infected with computer viruses or Trojan horses. Likewise, games may distract employees from their assigned duties. Games may additionally create an inappropriately playful and informal atmosphere that the organization sees as un business like.

2.2 Incidental Personal Use of Business Systems Permissible:

Jindal SAW Limited information systems are provided for, and must be used only for business purposes. Incidental personal use is permissible if the use: (a) does not consume more than a trivial number of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, and (c) does not pre-empt any business activity. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a meeting etc.

2.3 Personal Use of Jindal SAW Limited Internet Facilities only on Personal Time:

Jindal SAW Limited (JSAW) management encourages employees to explore the Internet, but if this exploration is for personal purposes, it must be done on personal, not JSAW time. Likewise, news feeds, discussion groups, games, and other activities which cannot definitively be linked to an individual's job duties must be performed personally, not JSAW time.

2.4 Permissible Uses of Jindal SAW Limited Information:

Jindal SAW Limited information must be used only for the business purposes expressly authorized by management.

2.5 Personal Use Time Limit and Prohibited Activities:

Incidental personal use of Jindal SAW Limited computer systems is permissible if this use is restricted to an hour or less per week. Such personal use must not include creation or distribution of chain letters, exchanging information which might be considered indecent, such as accessing or subscribing to pornographic sites, receipt or forwarding of jokes, moonlighting or searching for another job, participation in gambling activities, or engagement in political or charitable activities.

2.6 Disclaimer of Responsibility for Damage to Data and Programs:

JSAW uses access control and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, monitor, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. JSAW disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

2.7 Gaining unauthorized Access via Jindal SAW Limited Information Systems:

Employees using Jindal SAW Limited information systems are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. Likewise, employees are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

2.8 Prohibition against exploiting Systems Security Vulnerabilities:

Users must not exploit vulnerabilities or deficiencies in information systems security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted. All such vulnerabilities and deficiencies should be promptly reported to the Manager of Information Technology.

3. BACK-UP POLICY

3.1 Periodic Back-Up:

All sensitive, valuable, or critical information residents on JSAW computer systems or Network Drives must be periodically backed-up. Such back-up processes must be performed at least fortnightly. All end-users are responsible for making at least one current back-up copy of sensitive, critical, or valuable files. These separate back-up copies should be made each time that a significant number of changes are saved. User-generated back-ups must be periodically stored off-site in a physically secure location. Selected files from back-ups must be periodically restored to demonstrate the effectiveness of every back-up process.
SAP Backup process is different from the Normal user Data Backup Process, and it's separately maintained.

3.2 Periodic and Supplementary Backups required for Portable Computers:

Theft of portable computers is so common, employees using these computers must make backups of all critical information prior to taking out-of-town trips. These backups should be stored elsewhere than the portable computer's carrying case. This precaution supplements the periodic backups that must otherwise be made.
All end-users are responsible for making at least one current backup copy of critical files. These separate backup copies should be made each time that a significant number of changes are saved.

3.3 SAP Server Backup Policy

JSAW SAP server has Daily Incremental, and every 15 days full Backup policy configured.

4. ELECTRONIC MAIL POLICY

4.1 JSAW Property:

As a productivity enhancement tool, JSAW encourages the business use of electronic communications (notably the Internet, voice mail, electronic mail, and fax). Electronic communication systems and all messages generated on or handled by electronic communication system, including back-up copies, are considered to be the property of JSAW.

4.2 Authorized Usage:

JSAW electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial number of resources, (b) does not interfere with worker productivity, and (c) does not pre-empt any business activity. Users are forbidden from using JSAW electronic communication system for charitable endeavors, private business activities, or amusement/entertainment purposes. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

4.3 Respecting Privacy Rights:

Except as otherwise specifically provided employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. JSAW is committed to respecting the rights of its employees, including their reasonable expectation of privacy. JSAW also is responsible for servicing and protecting its electronic communication networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

4.4 Using an Electronic Mail Account assigned to Another Individual:

Employees must not use an electronic mail account assigned to another individual to either send or receive messages. If there is a need to read another's mail (while they are away on vacation for instance), message forwarding, and other facilities must instead be used.

4.5 Sender Contact Information must be included in Electronic Mail:

To facilitate communications and to properly identify the sending party, all outbound electronic mail sent using JSAW information systems must contain the sender's details.

4.6 No Guaranteed Message Privacy:

JSAW cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depend on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

4.7 Forwarding Electronic Mail to an External Network Address:

Unless the information owner/originator agrees in advance, or unless the information is clearly public in nature, employees must not forward electronic mail to any address outside JSAW's network. Blanket forwarding of electronic mail messages to any outside address is prohibited unless written permission from the Information Technology Manager has first been obtained.

4.8 Forwarding externally provided Electronic Mail Messages:

Employees must not create their own, or forward externally provided electronic mail messages which may be considered to be harassment or which may contribute to a hostile work environment. Among other things, a hostile work environment is created when derogatory comments about a certain sex, caste, religion or nationality are cast.

4.9 Users must not employ Electronic Mail Systems as a Database:

Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Stored electronic mail messages may be periodically expunged by system administrators, mistakenly erased by users, and otherwise lost when system problems occur.

Exception Caveat: This is applicable to all personnel other than exceptional cases as authorized by the HEAD IT.

4.10 Privacy Expectations and Electronic Mail:

Employees must treat electronic mail messages and files as private information. Electronic mail must be handled as a private and direct communication between a sender and a recipient.

4.11 Authorizations to read Electronic Mail Messages of other Employees:

When the JSAW Information Systems Security Cell agrees to it, electronic mail messages flowing through Jindal SAW Limited systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons. Unless electronic mail monitoring tasks have been specifically delegated by the above-mentioned managers, all employees must refrain from this activity

4.12 Message Content Restrictions for Jindal SAW Limited Information Systems:

Employees are prohibited from sending or forwarding any messages via Jindal SAW Limited information systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Employees are also prohibited from sending or forwarding messages or images via Jindal SAW Limited systems that would be likely to offend on the basis of race, gender, national origin, religion, political beliefs, or disability.

4.13 Notification of Content Monitoring for Electronic Mail Transmissions:

JSAW routinely employs automatic electronic mail content scanning tools to identify selected keywords, file types, and other information. Users should restrict their communications to business matters in recognition of this electronic monitoring

4.14 Integrity of Forwarded Mail

Contents of any mail that are forwarded must not be changed. If it has been changed, the same should be mentioned in the mail.

4.15 Reporting Offensive Electronic Mail Messages to Originator and HR:

Employees are encouraged to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications. If the originator does not promptly stop sending offensive messages, employees must report the communications to their manager and the Human Resources Department.

4.16 Forwarding is appropriate Response to Junk Email (SPAM):

When employees receive unwanted and unsolicited email (also known as SPAM), they must refrain from responding directly to the sender. Instead, they should forward the message to the system administrator who will take steps to prevent further transmissions.

4.17 Electronic Mail Messages are JSAW Records:

Jindal SAW Limited electronic mail system is to be used only for business purposes. All messages sent by electronic mail are Jindal SAW Limited records. JSAW reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. Supervisors may review the electronic mail.

Communications of employees they supervise to determine whether they have breached security, violated JSAW policy, or taken other unauthorized actions. JSAW may also disclose electronic mail messages to law enforcement officials without prior notice to the employees who may have sent or received such messages.

4.18 Personal Use of Electronic Mail Systems:

Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for- profit outside business activity, and must not potentially embarrass the JSAW.

4.19 Prohibition against use of scanned Hand-Rendered Signatures:

Employees must not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

4.20 Inbound Attachments To Internet Electronic Mail Prohibited:

Attachments to inbound Internet electronic mail messages sent to JSAW users will be automatically deleted. If a formatted file, an executable program, or some other non-text message must be sent, other methods such as FTP must instead be employed.

All inbound Word attachments must be in .rtf or .pdf format. Messages that are not in these formats shall be automatically quarantined, and an automatic return advisory shall be sent to the sender of the original message.

4.21 Handling Information about Security:

Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Information Systems Department. Users are prohibited from utilizing JSAW systems to forward such information to other users, whether the other users are internal or external to JSAW.

4.22 Purging Electronic Messages:

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas after a certain period -- generally six months.

5. ANTIVIRUS POLICY

5.1 Users must not attempt to eradicate Computer Viruses:

A computer virus is an unauthorized program, which replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. The symptoms of virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system. Because viruses have become very complex, users must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately shut-down the involved computer, disconnect from all networks, and call the systems dept.

5.2 Prohibition against downloading Software from Third Party Systems:

Employees must not download software from dial-up electronic bulletin board systems, the Internet, or any other systems outside JSAW. This prohibition is necessary because such software may contain viruses, worms, Trojan horses, and other software, which may damage JSAW information and systems

5.3 Testing for Viruses prior to use on JSAW Systems:

To prevent infection by computer viruses, employees must not use any externally-provided software from a person or organization other than a known and trusted supplier. The only exception to this is when such software has first been tested and approved by the Information Security Department or a local information security coordinator.

5.4 Required Process for Checking Software downloaded from Internet:

Software down-loaded from non-JSAW sources via the Internet may contain a virus (or similar programs such as worms or Trojan horses). Before such software is decompressed, users must log-out of all servers and terminate all other network connections. Then -- before it is executed -- the software must be screened with an approved virus detection package. If a virus is detected, the systems Department must immediately be notified, and no further work on this workstation may take place until the virus has been shown to be eradicated. If the software contains a virus, the damage will then be restricted to the involved workstation.

5.5 Virus Checking required for all externally supplied Floppy Disks:

Externally supplied floppy disks may not be used on any JSAW personal computer (PC) or local area network (LAN) PC/server unless these disks have first been checked for viruses and received a certification indicating that no viruses were found.

5.6 Virus Checking required for all external Laptops/Computers:

External computers/Laptop of Non-Jindal employee is prohibited to connect to JSAW local area network (LAN) or PC/server. The special permission is given to case-to-case basis for specified period in unavoidable circumstances. In such cases the Laptop/Computers should be checked for viruses using our standard Antivirus before connecting to JSAW network.

5.7 Prohibition against Programs consuming excessive System Resources:

Computer users must not run or write any computer program or process, which is likely to consume significant system resources or otherwise interfere with JSAW business activities.

5.8 All User involvement with Computer Viruses Prohibited:

Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any JSAW computer, network, or information. Such software is known as a virus, bacteria, worm, Trojan horse, and similar names.

6. PORTABLE COMPUTERS

Employees in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing "restricted" or "confidential" JSAW information must not leave these computers unattended at any time unless the information is stored in encrypted form.

To prevent unauthorized disclosure, employees in the possession of transportable computers containing unencrypted "restricted" or "confidential" JSAW information must not check these computers in airline luggage systems, with hotel porters, etc. These computers must remain in the possession of the traveler as hand luggage.

Whenever "restricted" or "confidential" information is written to a floppy disk, magnetic tape, smart card, or other storage media, the storage media must be suitably marked with the highest relevant sensitivity classification. When not in use, this media must be stored in locked safe, locked furniture, or a similarly secured location.

7. REMOTE PRINTING

Printers must not be left unattended if "restricted" or "confidential" information is being printed or will soon be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted if the area surrounding the printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

8. WEB PRIVACY POLICY

8.1 Web Page Changes:

Employees may not establish new Internet web pages dealing with JSAW business, or make modifications to existing web pages dealing with JSAW business, unless they have first obtained the approval of the Systems/ Corporate communication Department. Modifications include the addition of hot-links to other sites, updating the information displayed, and altering the graphic layout of a page. This Corporate communication Department will make sure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected with adequate security measures.

8.2 Unofficial Web Pages permitted only by Contract:

Unofficial web pages dealing with JSAW products or services are prohibited, unless the sponsor of these home pages has a contract signed with JSAW. Employees who notice a new Internet reference to JSAW products and/or services are requested to promptly notify to Corporate Communication head and HEAD IT.

8.3 JSAW blocks certain non-business Internet Web Sites:

JSAW information systems routinely prevent users from connecting with certain non-business web sites. Employees using JSAW information systems who discover they have connected with a web site that contains sexually explicit, racist, or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.

9. INTERNET POLICY

9.1 Applicability:

This policy applies to all employees (employees, contractors, consultants, etc.) who use the Internet with JSAW computing or networking resources, as well as those who represent themselves as being connected in one way or another with JSAW. All Internet users are expected to be familiar with and comply with this policy. Violations of this policy can lead to revocation of system privileges and/or disciplinary action upto and including termination.

9.2 Prior Management Approval:

Access to the Internet (aside from electronic mail) will be provided to only those employees who have a legitimate need for such access. The ability to surf the web and engage in other Internet activities is not a fringe benefit to which all employees are entitled.

9.3 Virus Checking:

All non-text files (databases, software object code, spreadsheets, formatted word-processing package files, etc.) downloaded from non-JSAW sources via the Internet must be screened with virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed-up. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine. Downloaded files must be decrypted and decompressed before being screened for viruses. Separately, the use of digital signatures to verify that unauthorized parties have not altered a file is recommended, but this does not assure freedom from viruses.

9.4 Expiration of User-IDs on Internet Accessible Computers:

User-IDs on Internet accessible computers must be set to expire six months from the time they are established. Renewals of these user-IDs are permissible, but must be restricted to six-month intervals.

9.5 Internet Discussion Group and Chat Room Participation Forbidden:

Unless expressly authorized by the Corporate Communication department, when using JSAW information systems, all JSAW employees are forbidden from participating in Internet discussion groups, chat rooms, or other public electronic forums.

9.6 Internet Representations about JSAW Products & Services:

Employees must not advertise, promote, present, or otherwise make statements about JSAW products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the Corporate Communication /legal & Marketing Departments.

9.7 Respecting the Intellectual Property Rights of Others on the Internet:

Although the Internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To this end, employees using JSAW systems must for example (1) repost material only after obtaining permission from the source, (2) quote material from other sources only if these other sources are identified, and (3) reveal internal JSAW information on the Internet only if the information has been officially approved for public release.

9.8 Push Technology:

Automatic updating of software or information on JSAW computers via background "push" Internet technology is prohibited unless the involved vendor's system has first been tested and approved by the Internet Group within the Information Systems Department. While powerful and useful, this new technology could be used to spread viruses, and cause other operational problems such as system unavailability.

10. INFORMATION CONFIDENTIALITY

10.1 Message Interception:

Wiretapping and other types of message interception are straightforward and frequently encountered on the Internet. Accordingly, JSAW secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet. For the same reasons, Internet telephone services must not be used for JSAW business unless the connection is known to be encrypted.

11. PUBLIC REPRESENTATIONS

11.1 Appropriate Behavior:

To avoid liability, defamation of character, and other legal problems, whenever any affiliation with JSAW is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, employees must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited

11.2 Disclosing Internal Information:

Employees must not publicly disclose internal JSAW information via the Internet that may adversely affect JSAW's stock value, customer relations, or public image unless the approval of the Head of Corporate communication or Public Relations or a member of the top management team has first been obtained. Such information includes business prospects, products now in research and development, product performance analyses, product release dates, internal information systems problems, and the like. Such information must be cross-referenced with the Public Affairs Department.

12. INTELLECTUAL PROPERTY RIGHTS

12.1 Copyrights: (Flag for Management Comment)

JSAW strongly supports strict adherence to software vendors license Agreements. When at work, or when JSAW computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with JSAW work and are therefore prohibited. Similarly, the reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other materials must be done only with the permission of the author/owner. Employees should assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" as well as specifics about the source of the information (author names, URLs, dates, etc.).

13. PERSONAL USE

13.1 Personal Use:

JSAW management encourages employees who have been granted Internet access to explore the Internet, but if this exploration is for personal purposes, it must be done on personal, not JSAW time. Likewise, games, news groups, and other non-business activities must be performed on personal, not JSAW time. Use of JSAW computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no JSAW business activity is pre-empted by the personal use. Employees must not employ the Internet or other internal information systems in such a way that the productivity of other employees is eroded; examples include chain letters and broadcast charitable solicitations.

13.2 Blocking Sites:

JSAW firewalls routinely prevent users from connecting with certain non-business web sites. Employees using JSAW computers who discover they have connected with a web site that contains sexually explicit, violent, or other potentially offensive material must immediately disconnect from that site and subsequently inform to System Administrator for corrective action. The ability to connect with a specific web site does not in itself imply that users of JSAW systems are permitted to visit that site.

13.3 Blogging and Social Networking

Blogging and Social Networking by employees, whether using JSAW's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of JSAW's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate JSAW's policy, is not detrimental to JSAW's best interests, and does not interfere with an employee's regular work duties. Blogging from JSAW's systems is also subject to monitoring.

JSAW's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any JSAW confidential or proprietary information, trade secrets or any other material covered by JSAW's Confidential Information policy when engaged in blogging.
Employees shall not engage in any blogging/Social Networking that may harm or tarnish the image, reputation and/or goodwill of JSAW and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by JSAW's Non-Discrimination and Anti-Harassment policy.

Employees may also not attribute personal statements, opinions or beliefs to JSAW when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of JSAW. Employees assume all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, JSAW's trademarks, logos and any other JSAW intellectual property may also not be used in connection with any blogging activity.

14. PRIVACY EXPECTATIONS

14.1 Management Review:

At any time and without prior notice, JSAW management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through JSAW Computers. Such management access assures compliance with internal policies, assist with internal investigation and assist with the management of JSAW information systems.

14.2 Junk Email:

When employees receive unwanted and unsolicited email (also known as spam), they must refrain from responding directly to the sender. Instead, they should forward the message to the email administrator at JSAW who can then take steps to prevent further transmissions. To respond to the sender would be indicate that the user-ID is monitored regularly, and this would then invite further junk email.

15 Physical Security for Computer Protection

15.1 Purpose

State office locations that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to;
security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors
at entrances, security guards, and fire protection. Information Security issues to be considered are:

Unlawful access may be gained with the intent of theft, damage, or other disruption of operations.

Unauthorized and illegal access may take place covertly (internal or external source) to steal, damage, or otherwise disrupt operations.

Destruction or damage of physical space may occur due to environmental threats
Such as fire, flood, wind, etc.

Loss of power may result in the loss of data, damage to equipment and disruption of operations.

15.2 Scope

This policy addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by the State of Vermont, including offices, data centers and similar facilities that are used to house such resources.

15.3 Policy

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

15.4 Use of Secure Areas to Protect Data and Information

Use physical methods to control access to information processing areas.
These methods include, but are not limited to, locked doors, secured cage areas, vaults, ID cards, and biometrics.
Restrict building assess to authorized personnel.
Identify areas within a building that should receive special protection and be designated as a secure area. An example would be a server room.
Use entry controls.
Security methods should be commensurate with security risk.
Ensure that physical barriers are used to prevent contamination from external environmental sources. For example: Water tight walls in flood zones. Proper ventilation in areas exposed to chemical vapors.
Compliance with fire codes
Installation, use and maintenance of air handling, cooling, UPS and generator backup to protect the IT investment within data rooms.

15.5 Physical Access management to protect data and information

Access to facilities that house critical state IT infrastructure, systems and programs must follow the principle of least privilege access. Personnel, including full and part-time staff, contractors and vendors' staff should be granted access only to facilities and systems that are necessary for the fulfillment of their job responsibilities.

The process for granting physical access to information resources facilities must include the approval of the CIO, or his or her designee. Access reviews must be

Conducted at least quarterly, or more frequently depending on the nature of the systems that are being protected. Removal of individuals who no longer require access must then be completed in a timely manner.

Access cards and keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.

Security clearance for visitors. This could include, but is not limited to, a sign in book, employee escort within a secure area, ID check and ID badges for visitors.

16 Change Management

Definition and process

IT Change Management is the process of requesting, developing, approving and implementing a planned or unplanned change within the IT infrastructure. It begins with the creation of a Change Request and it ends with the satisfactory implementation of the change and communication of the result of the change to all interested parties.

The Change request is received on emails (on a central ID for SAP related issues) after due approval from concerned process owner at location/Corp office. The technical feasibility is done by SAP/IT teams. If feasible and all required approvals are in placer than the change is incorporated and tested by IT team for initial testing, and then it is released to the concerned users for final testing.

17 Removable Media Access

Jindalsaw Ltd has prohibited using flash drives to store information of any kind Mass Storage but System Administrator can only allow Mass Storage device after respective HOD/IT Head Approval for a specific period.

18 Security and Hardening Process

Before allocating any new assets, IT person will update all necessary patches and all Domain based desktop, Laptops and Servers would be properly patch from manual or any available update software.

19 Cybersecurity Incident Response Checklist

(i)Focus Response Efforts with a Risk Assessment (ii) Identify Key Team Members. (iii) Define Incident Types and Thresholds. (iv)Inventory Your Resources and Assets. (v) Recovery Plan Hierarchies and Information Flow. (vi)Prepare an Incident Event Log.

20 Software usage Policy

The purpose of the Software Usage Policy is to ensure that employees are properly trained on appropriate procedures surrounding safe and legal use of company-owned software.
Installing unauthorized software on a computer system, workstation, or network server within an organization can lead to potential system failures, system degradation or viruses. Unauthorized installations also place its employees at risk for civil and criminal action, which can result in punitive measures imposed on all involved parties.

21 Log Management

The Audit trail of all financial transactions is maintained in SAP and is available for a duration as per legal requirement.

22 Asset Management and other IT Process and Policies

Asset would be maintained manually or according to any available management software.

1. **Make, Model and Configuration**
   To achieve standardization in Price, Service and Replacement benefits the make, model and configuration of various IT equipment's would be finalized by Corporate IT from time-to-time. Corporate Purchase would then finalize the best price for the various models and arrange to be supplied and supported across all locations.
   In addition for Laptops, the allocation of a particular make, model and configuration would depend on the nature of work of the personnel. Local IT Head would recommend the same to CIO-Corporate for final approval, for all.
2. **Requisition Process**
   The duly approved requisition for a Laptop, Desktop, printer and peripherals should be submitted to Local IT.
   For new joining at HOD level, HR would initiate the requirement and complete the authorization procedure.
3. **Allocation and Procurement**
   All requisitions would be screened by IT Department and if allocation is justified as per this policy, the requisite IT equipment would be allocated. It may be noted that these would be allocated either from the available stocks or new procurement.

4. Parting employees

All parting employees need to return the IT equipment’s issued to them, with local IT department, on or before the last date of working. HR is to process the full and final settlement of the person, only after clearance from IT. Where material is returned in damaged condition, the cost of repairs / replacement is to be charged to the person concerned.

5. Usage, Security and Audit

All IT equipment is provided to facilitate official working and one must take utmost care of the same. Some of the points to be ensured are as follows:

1. The Laptop / Desktop are issued by IT department with all standard software and applications preinstalled, as per the nature of work of the person. Downloading and installing any other software, without written consent from IT, is not allowed.
2. Personnel, who access the Internet and Email using data cards or public networks, must be extra careful not to access or download from any sites that contain inappropriate material. These include unlicensed software, games, music and videos. Further accessing or downloading or circulating any pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment, is not allowed. If you accidentally browse to an offensive website, click ‘back’ or close the window straight away. Kindly note that your laptops / desktops identification can be tracked for the sites accessed and emails sent.
3. JSAW uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to: (1) restrict or revoke any user's privileges, (2) inspect, monitor, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the user.
4. Employee using Jindal SAW Limited information systems are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. Likewise, employees are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access. Similarly unauthorized access to classified data, copying it to pen-drive and / or emailing the same is not permitted.
5. The laptop / desktop must be password protected to ensure authorized access only by designated user. The password is not to be shared with anyone. It is further recommended that the password is changed frequently.

6. Avoid leaving your laptop / desktop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before moving away from it.

7. Take regular backup of your data including email data, either on your own or through IT. This activity must be done, at-least once every quarter.

8. IT would periodically take the laptop / desktop for servicing. You are required to co-operate and handover the same whenever stated to do so.

9. Be sure before opening any email attachments, since these are the primary source for virus infection. Delete emails that are not received from a known or trusted source.

10. When downloading or copying a file from any external source the antivirus would initiate a scan. Never stop this action.

    Respond immediately to any virus warning message on your computer, or if you suspect a virus by contacting the IT Help Desk. Do not forward any files or upload data onto the network if you suspect your laptop / desktop might be infected.

Laptop users should additionally note:

11. Do not loan your laptop or allow it to be used by others such as family and friends.

12. Do not leave the laptop unattended in the vehicle, hotel room, conference hall or any other outside location, even for a short while. Also be extra vigilant at restaurants, railway stations, trains and airports.

13. Laptops normally have smaller keyboards, displays and pointing devices as compared to desktops and hence are less comfortable to use. This often leads to strains. It is advised that you take periodic breaks while using your laptop. Wherever possible, place the laptop on a table and sit comfortably in an appropriate chair to use it.

14. Most laptops have an exhaust fan at the bottom. Hence never use a laptop placing it on the bed or pillow, as the exhaust would get blocked and lead to excessive heating. This would damage the laptop. At times excessive heating leads to short circuit and fire.

15. Lock the laptop away, when you are not using it, preferably in a strong cupboard.

16. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.

17. Keep a note of the make, model and serial number of your laptop. In the unfortunate event of it getting lost or stolen, notify the Police immediately and ensure that the make, model and serial number are mentioned in the FIR. Also inform the IT Help Desk as soon as possible.

6. **Replacement**

A request for replacement would be entertained subject to the following:

a. The IT equipment is no longer serviceable due to natural wear and tear
b. The system is outdated, due to changes in technology.
c. Repairing the same is not economical.
d. It does not support applications required for effective working.

All replacement requests against

physical damages / lost / stolen would need fresh approvals. IT can recommend a change in the cost of repairs / replacements to be borne by the executive to whom the equipment was allotted.

7. **Withdrawal**

Any IT equipment that is issued to a person would be withdrawn under the following circumstances

a. It is not used for the purposes for which it was provided.
b. There is a change in the job of the person and the new assignment does not require the same.

8. **Other**

This policy is subject to alteration / modification from time to time as per need.