ISMS (Information Security Management System) Policy Manual

AS PER INTERNATIONAL STANDARD

ISO 27001:2013

Revision History

Date	Version	Author	Description	Approver
25-Feb-2021	1.0	Kedar Bhise	Initial Version	Mark Khabe

INFORMATION SECURITY POLICY

Ref. Control Section: --A5.1

Control A.5.1	Information Security Policy
Control A.5.1.1	Policies for Information security
	Prime BPM Information Security Policy document is prepared and approved by the management. The document is classified as Internal and circulated to all employees and relevant external parties. PURPOSE The purpose of the Policy is to protect the information assets of Prime BPM from all threats, whether internal or external, deliberate or accidental. OBJECTIVE Prime BPM's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions. Prime BPM shall ensure that all information that is disseminated or produced by them has absolute integrity. Prime BPM shall ensure that all relevant information is managed and stored with appropriate levels of confidentiality and that correspondingly relevant procedures are developed and applied in this regard. **The Information security Policy defined by the top management:** The Prime BPM information security policy has been updated in the ISMS Manual document. The ISMS objectives have been updated in the ISMS Manual.
Control A.5.1.2	Review of policies for information security
	The Prime BPM information security policy shall be reviewed at least on an annual basis or whenever there are major changes to the system. CISO will co-ordinate and take inputs from various document / policies owner and present in the MRM, where it will be approved or send an email to the approving authority and it will be approved over email or present the hard copies to the approving authority and obtain signature of approval on the list of documents presented.

INTERNAL ORGANIZATION

Ref. Control Section: --A6.1

Control A.6.1	Internal Organization
Control A.6.1.1	Information security Roles and Responsibilities
	All information and assets of Prime BPM are owned by defined key members within the organization. Prime BPM has defined levels of protection and owners to ensure that each owner with specific roles and responsibilities be guided by business definitions or regulatory requirements and specifications of defined Prime BPM security Model. Each owner shall be responsible for information and asset classification and determine the applicable controls. Responsibilities for personnel in different categories individually have been defined and assigned. Human Resource Department with inputs from CISO shall define security roles and responsibilities of employee, contractors and third-party users. Their roles and responsibilities shall **be reviewed every year** by CISO. *Refer ISMS Manual for detailed Roles and Responsibilities.*
Control A.6.1.2	Contact with Authorities
	Prime BPM uses the services of law enforcement authorities to protect its assets from natural and unnatural calamities. List of contacts of law enforcement authorities is available with Admin department and co-ordinate with these authorities in emergencies.
Control A.6.1.3	Contact with special interest groups
	Prime BPM encourages its employees to be part of special security forums and professional associations to keep abreast with the latest security breaches, threats and technology developments, which would improve knowledge about the best practices ensuring the learning's are inculcated in their function and workplace. It has been made mandatory that no information internal to the organization shall be exchanged in these forums. Employees will inform the CISO of their membership to such groups and have to get approval for disclosing any non-public information to such forum or group. Refer: List of relevant special interest groups
Control A.6.1.4	Information security in Project Management
	Information security is integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as

part of a project. This applies to any project regardless of its character, e.g., a project for a core business process, IT, facility management and other supporting processes.

The project management methods in use require that:

a) information security objectives are included in project objectives;

b) an information security risk assessment is conducted at an early stage of the project to identify necessary controls and repeated in case of changes to the project.

c) for identified information security risks, measures are derived and taken into account in the project.

d) the measures thus derived are reviewed regularly during the project and re-evaluated in case of changes to the evaluation criteria.

e) the project is then classified by the CISO into high, medium and low based on the criteria as mentioned below:

Classification for each individual project is determined based on the impact in case of breach of confidentiality, integrity and availability.

Each project is given a rating of High Medium or Low against Confidentiality, Integrity and Availability.

This rating is converted into numbers by giving high a 3 rating, medium a 2 rating and low a 1 rating.

Guidelines for rating Confidentiality, Integrity and Availability

Confidentiality

This means that ensuring that information is accessible only to those authorized to have access.

Confidentiality Rating.

High-Secret. The loss of confidentiality will gravely injure organizational interests

Medium-Confidential-Business information, loss of which can affect the business in terms of opportunity costs or injury organization interests

Low-Unclassified. Unclassified –Unimportant or basic information, hence no loss Integrity

Integrity Rating.

High-The loss of integrity gravely injures the core of the organization

Medium--Loss of integrity can affect organization interests and loss in terms of opportunity costs

Low-No issue as no damage is caused

Availability

This means ensuring that authorized users have access to information and associated assets when required

Availability Rating.

High-Critical Service and loss of availability causes operations to come to a complete halt

Medium-Loss of availability causes moderate degradation in productivity

Low-No impact

Depending on the computed number for the C, I, A ratings the criticality of the project is assessed as follows:

	<table><tr><th>Ratings</th><th>Project classification</th></tr><tr><td>7 to 9</td><td>High</td></tr><tr><td>4 to 6</td><td>Medium</td></tr><tr><td>3</td><td>Low</td></tr></table> f) information security is part of all phases of the applied project methodology. An information Security Project Plan checklist is filled by the CISO along with the project manager to cover the above points and signed off before the initiation of the project. Software development projects will be managed using suitable project management tools like, Azure Boards, Trello etc.
Control A.6.1.5	Segregation of Duties
	Duties have been segregated, where ever possible to eliminate negligent or deliberate system misuse. IT team members are cross-trained so that expertise / access for a certain system do not lie with a single employee. Wherever possible, Maker / Checker process is implemented to ensure that the creator is not the approver and that there is an independent review done before finalizing and work product or approving any process. Primary and Secondary responsibilities for critical information security roles are documented and followed.

MOBILE DEVICES

Ref. Control Section: --A6.2.1

Control A6.2	**Mobile devices and teleworking**
	Prime BPM clearly understands the importance of Security and applicable controls that need to be maintained while information processing facilities are being accessed, processed, communicated or managed by external parties for business needs.
Control A.6.2.1	Mobile Device policy
	Refer: Mobile Device Policy document
Control A.6.2.2	Teleworking
	Only if Prime BPM approves and is able, to provide suitable teleworking facilities, may a member of staff undertakes teleworking and only in cases where: • It is Prime BPM that requires the member of staff to undertake teleworking or it has been approved for the member of staff to adopt a formal flexible working arrangement. Staff must also be authorised by their Head of Department to undertake teleworking as distinct from other remote working arrangements. This authorisation must be recorded by the department. The teleworking authorisation process should involve an assessment of information security risk taking into account several factors: criticality of the information assets being accessed, confidentiality of information being handled and suitability of the teleworking technology and location. Those providing or supporting remote access facilities must do so in cooperation and with approval of IT Services. Arrangements must be in place to ensure that any Prime BPM teleworking solutions that should be provided are fully supported and maintained. IT Team must ensure, on termination of the arrangement, the secure return or disposal of all equipment and information, in electronic and paper form, held by the teleworker. Any software used as part of Prime BPM teleworking solution must be appropriately licensed. Any teleworking equipment which provides remote access to the Prime BPM network, and the authentication method that it uses to access Prime BPM resources, must be approved by CISO / Top Management.

	Provision and support of teleworking must reliably implement comprehensive information security measures. Where it is unavoidable that a teleworker must handle confidential information, they must be provided with a computer incorporating full disk encryption and where necessary file encryption tools Staff, provided with computing and communications equipment for teleworking specifically to protect the security of confidential information, must not put the information at risk by using other less secure equipment. Teleworking equipment provided by Prime BPM may only be modified or replaced if that has been authorised. Teleworking equipment supplied by Prime BPM is only to be used by Prime BPM staff, particularly since others are not bound by Prime BPM agreements and policies. Teleworking staff must ensure that adequate backup procedures for any information held offsite are implemented. It would normally, however, be preferable to remotely access data that is held onsite and already subject to routine backup. Where absolutely necessary to handle confidential hardcopy documents they should be kept in locked cabinets when not attended (clear desk policy), sent by special delivery post, delivered by hand where possible and disposed of by shredding.

HUMAN RESOURCE SECURITY

Ref. Control Section: --A7

Control A.7.1	**Prior to employment**
	Prime BPM runs the new joiner through security policy guidelines to sensitize on the understanding of the security aspects and also the risk arising out of human errors, theft, fraud and misuse of IT facilities. Prime BPM has made it necessary to ensure that their users are aware of information security threats and weaknesses, and are equipped to support Prime BPM Security Policy during the course of their normal work.
Control A.7.1.1.	Screening
	Verification checks are carried out on all selected job applicants by the HR department. This includes identity checks, which are carried out through driving license verification or any Government provided ID proof of all Prime BPM employees. In addition, all the documents are verified during the on-boarding of the employee. Verification checks apart from the ones mentioned above can be performed for a candidate under the following reasons: • On Client requirement • On request by Department Head Refer: Background Verification Policy
Control A.7.1.2	Terms and conditions of employment
	While defining the terms and conditions of employment/ job contract, HR team and CISO shall ensure that employee/third party agree and sign the terms and conditions of the employment contract, stating clearly their responsibilities for Information security of Prime BPM. All employees / contract staff / temporary staff are required to sign off a non-disclosure agreement at the time of joining. These agreements should be reviewed when there are changes to terms of employment or contract.
Control A.7.2	During Employment
	Prime BPM shall ensure that all employees, contractors and third-party users are aware of security threats and concerns and shall be equipped to support Prime BPM security policy thereby minimizing the chances of human error.
Control A.7.2.1	Management Responsibilities

	CISO shall ensure that employees, contractors and third-party users are applying security in their day-to-day operations in accordance with established Security policies and procedures of Prime BPM. All shall be briefed on information security roles and responsibilities prior to granting access to information and information processing facilities. All shall be made to understand the seriousness of security concerns through training and awareness programs periodically.
Control A.7.2.2	Information Security awareness, education and training
	Information Security awareness trainings shall be given to new staff (Employee, third party) who shall be provided access to IT systems, information and assets. These trainings are a part of the induction program of a new employee. The trainings shall include at a minimum: ☞ Management's commitment to information security ☞ Security policy of the organization and compliance towards the same ☞ Personal accountability for information security ☞ Security related do's and don'ts ☞ Security incident reporting Information security awareness refresher session is conducted once in a year.
Control A.7.2.3	Disciplinary Process
	A formal disciplinary process is put in place to deal with employees who have allegedly violated company security policies and procedures. Refer: Disciplinary Process
Control A.7.3	Termination or change of employment
	Prime BPM shall take necessary steps to ensure that its employees, contractors and third-party users exit/change their employment/role in an orderly manner so that the organizational interests are not affected.
Control A.7.3.1	Termination Responsibilities
	Prime BPM shall invoke termination process based on the following: • If an employee / 3rd party / service vendor has violated the clauses mentioned in the signed agreements. • When an employee remains absent from office for more than the applicable period as per the position within Prime BPM. In such cases, HR shall instruct the IT team to disable user/e-mail accounts of the user for the period of absence. The account shall be disabled / locked out after 3 days of inactivity after the

	conformation from the Reporting Manager to HR. If an employee's employment is terminated, HR informs the IT Team, who will take the necessary actions. In case of senior executive, the reporting head may transfer the required and or important data to the designated person (new recruit, a peer or a senior officer). • Resignation of an employee, the HR team sends email to IT and concerned departments for disabling of user Ids of various IT resources like email, system, Azure Boards etc. on the Last working day. The individual shall be debriefed with respect to ongoing responsibilities for the confidentiality of Prime BPM by HR during EXIT interview.

ASSET MANAGEMENT

Ref. Control Section: --A8

Control A.8.1	Responsibility for assets
	Prime BPM has clearly defined asset owners who shall classify and ensure the level of protection for its organizational assets as per the criticality & risk assessment and maintain it.
Control A.8.1.1.	Inventory of assets
	Prime BPM asset inventory is maintained for each hardware, software / technology, personnel, service and informational asset. Every asset is labelled as per approved naming / labelling scheme. Inventory is maintained for following type of assets: • Physical assets • Information assets • Software / Technology assets • Paper documents • Services • People asset • Intangible assets
Control A.8.1.2	Ownership of asset
	Currently process owners are the owner of the assets of the organization
Control A.8.1.3	Acceptable use of assets
	Refer: Acceptable use of assets policy
Control A.8.2	Information Classification
Control A.8.2.1	Classification Guidelines
	Information belonging to or under the custody of the Company shall be classified based on sensitivity of information. The asset owner will classify information under their control as Confidential, Internal and Public. The definitions of the classifications are as follows: **Confidential** Information that is sensitive within the Company and intended for internal business use only by those with a need-to-know. **Internal** -. Generally available to employees within the respective functions and to employees within the organization on a need-to-know basis **Public** - Non-sensitive information available for public disclosure. **Refer**: Asset classification Policy
Control A.8.2.2	Information labelling & handling
	Refer: Asset classification Policy
Control A.8.2.3	Handling of Assets
	Refer: Asset classification Policy

Control A.8.2.4	Return of assets
	HR shall ensure all organization assets are returned from employees / contractors and third-party users upon termination and / or change of responsibility (transfer from one function to other) of employment, contract or agreement.
Control A.8.3	Media Handling
	To avoid interruptions to the business activities of Prime BPM, its media shall be controlled and physically protected. This is necessary to prevent unauthorized and unintended disclosure, modification, removal or destruction of assets. Appropriate procedures shall be established to protect paper documents and computer media from damage, theft, unauthorized access and misinterpretation.
Control A.8.3.1	Management of removable media
	At Prime BPM all information shall be stored on enterprise network storage environment, which are protected against any hardware malfunction / failure. Any access to removable media including hard disk, tape drive, USB, CD ROM or devices, printers, scanner, data cards or any other peripherals, shall be given with approvals of Department head or IT department. IT department shall monitor the usage of printer on constant bases and notify user in case the usage is high. Sensitive data shall not be stored on mobile data storage media (like external HDD, USB drive etc.) without a documented business necessity and description of mitigating controls approved in writing by the Department Head. All data storage media containing sensitive data must be both physically and logically secured. The approval must document the business reasons for accepting the risks to the data and a description of mitigating controls in place.
Control A.8.3.2	Disposal of media
	Media / assets that are marked for disposal after necessary approvals shall be disposed of securely as per the media disposal procedure. **Disposal of Hardcopy Records** **Hardcopy Disposal** - When disposed of, all secret, confidential, or private information in hardcopy form must be either shredded or incinerated. To ensure that documents are properly destroyed, only shredders approved by Prime BPM will be used to shred hardcopy records containing sensitive information. **Secure Information Containers** – Sensitive information that is no longer needed must be shredded within Prime BPM offices and never placed in trash bins, recycle bins, or other publicly-accessible locations. **Disposal of Electronic Media** **Storage Media Destruction** - Destruction of sensitive information captured on

	computer storage media must only be performed with approved destruction methods including shredders or by physical damaging the hard disk. **Disposal of Electronic Media Outside of Prime BPM** - All electronic media must be erased, or degaussed, or rendered unusable before leaving Prime BPM. **Disposal of Computer Equipment** **Used Component Equipment Release** - Before disposal, donation, or recycling, the Systems Department must validate that sensitive information has been removed from any information systems equipment that has been used for Prime BPM business. This validation process must take place before releasing such equipment to a third party. **Information and Equipment Disposal** – Systems Team is responsible for the disposal of surplus property no longer needed for business activities in accordance with procedures established, including the irreversible removal of sensitive information and licensed software. **Inventory of Decommissioned Computer and Network Equipment** - The Systems Department must maintain an inventory of all Prime BPM computer and network equipment that has been taken out of commission. This inventory must also reflect all actions taken to clear memory chips, hard drives, and other storage locations in this same equipment of all stored information. **Transfer of Hard Drives and Media** **Transfer of Hard Drives** - Before a hard drive is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access the data by ordinary means. All electronic media should be sanitized (low level formatting) according to Prime BPM procedures. **Transfer of Electronic Media** - Before electronic media is transferred from the custody of the current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible. **Attempted Recovery** – Attempts to recover deleted or sanitized data must only be done by specially trained personnel approved by Prime BPM management. Insofar as special recovery tools would have to be used by an individual to access the data erased by this method, any attempt by an individual to access unauthorized data would be viewed as a conscious violation of state or federal regulations and the Prime BPM Confidentiality Statement.
Control A.8.3.3	Physical media in transit
	When sending information through postal service or via courier, reliable couriers are used. Administration maintains a list of approved couriers and these couriers are used for information exchange. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturer's specifications. Special controls, like encryption, shall be adopted to protect sensitive information from unauthorized disclosure and modification.

ACCESS CONTROL

Ref. Control Section: --A9

Control A.9.1	Business requirements of Access control
	Prime BPM shall control access to information by establishing and documenting a procedure for access control and management. This shall be reviewed based on business and security requirements.
Control A.9.1.1	Access control policy
	All the Organization systems shall develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance. Refer: Access Control Policy
Control A.9.1.2	Policy on the use of network services
	Users shall be granted access to Network Services like Printing, File sharing and Network Applications by IT Team depending on business requirement. These services will have a restricted usage access to ensure information leakage possibility. Refer: Network Security Process
Control A.9.2	User access management
Control A.9.2.1	User registration and de-registration
	Human Resources Department shall forward information regarding all new employees to IT team for the creation of their local system ID and Gsuite ID. Users are provided with the capability to change their password on the login interface (after authentication). New users shall be acquainted with the Prime BPM organizational Security policy and access procedures and violation of any shall be taken seriously. Access privileges of users leaving the organizations shall be revoked as soon as Human Resources Department informs IT team as per the employee Exit process.
Control A.9.2.2	User Access provisioning
	Prime BPM has implemented User Access Management to control the access rights to information systems and services, to prevent unauthorized access to information systems. Process owners are responsible for providing access to users. This shall be applicable to all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

Control A.9.2.3	Management of privileged access rights
	The privilege allocation is only on need-to-know basis and shall be reviewed & documented bi-annually. All the privileged user passwords for Operating Systems, Databases, Applications, Network Equipment like routers, switches etc., are sealed in an envelope and kept in custody of CISO.
Control A.9.2.4	Management of secret authentication information of users
	Allocation of secret information is controlled through formal process. Passwords are frequently used secret information within Prime BPM. Passwords are assigned to individuals in a secure manner after verifying their identity. The Individual User IDs once assigned shall not be shared and users shall maintain their individual passwords and shall not reveal to anyone. The password acceptance shall be in line with the password policy defined by Prime BPM. As per the password policy, Prime BPM reviews the password policies of user's half yearly to ensure that there is no malicious use. *Refer: Password Policy*
Control A.9.2.5	Review of user rights
	Review of Users Access Rights Privileged user accounts / application access rights are reviewed bi-annually. Application/Data owner would be responsible for any change in access to the application/data for a user and the same change shall be communicated to the System Administrator for facilitating the access control change. Access to data, programs, and applications shall be immediately removed for employees who are transferred from the business unit for project needs. User access review should be performed for all user accounts on domain, email and Applications on a **bi-annual** basis. Further, documented process should be in place which defines the procedure to be followed in case of an unauthorized access to information system resources.
Control A.9.2.5	Removal or adjustment of access rights
	On receiving exit checklist / email from HR the IT team shall remove the access rights of the concerned personnel. In case employees are transferred from one project / function to other then the concerned process owners should raise request over email for de-activation / activation of access rights in the email, post which IT team will adjust the access rights accordingly.
Control A.9.3	User Responsibilities
	To prevent unauthorized user access and compromise or theft of information, every user has responsibilities to ensure the security of the information assets and also of the computing resources used by him/her and the data that they contain.
Control A.9.3.1	Use of secret Authentication information

	Passwords are frequently used secret information within Prime BPM. Passwords shall not be displayed in any environment (including on office walls, desks and workstations) at any time, including during sign-on procedures. The password use Policy defined by Prime BPM shall be strictly followed by existing staff as well as new employees joining in.
Control A.9.4	System and application access control
	Logical access to software and information shall be restricted to authorized users as defined by the process owners.
Control A.9.4.1	Information access restriction
	Users of application systems shall be provided access to information and application system functions based on individual business application requirements consistent with organizational information access policy.
Control A.9.4.2	Secure log-on Procedures
	IT Team will ensure that, • The system shall be setup such that every person using the system has to logon using a unique user id and password. • The system shall be configured not to display any help messages or error messages before the logon procedure is complete. • Inactive session shall be closed after a defined period of activity. The time period shall be defined by IT team and communicated as part of acceptable use guidelines of the system. The time period will define based on business requirement and risk assessment. • Limitation on the connection time shall be fixed by Prime BPM based on the demands of the clients and its usage frequency.
Control A.9.4.3	Password management system
	Password management shall be automated through system enforceable password policies, where ever feasible. *Refer: Password Policy*
Control A.9.4.4	Use of privileged utility programs
	The use of privileged utility programs that might be capable of overriding system and application controls shall be restricted and controlled.
Control A.9.4.5	**Access control to program source codes**
	The folders present to store the source code is provided with the access rights based on the roles played by the team.

CRYPTOGRAPHY

Ref. Control Section: --A10

Control A.10.1.1	Policy on use of cryptographic controls
	Prime BPM's policy on Cryptography is that appropriate encryption control measures are implemented to protect its sensitive or critical information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources. The objectives of this policy with regard to the protection of information system resources against unauthorised access are to: • Minimise the threat of accidental, unauthorised or inappropriate access to critical or sensitive electronic information owned by Prime BPM or temporarily entrusted to it by applying a proportionate level of encryption control • Minimise the network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources • Minimise reputation exposure, which may result in loss, disclosure or corruption of critical or sensitive information and breach of confidentiality **Data at rest:** • Approved encryption methods for data at rest • Any agreements for the exchange of personal, confidential and commercially sensitive data, whether transported manually or electronically (including an attachment to email), must specify security controls that reflect the sensitivity of the information involved and the risks to the data during its transfer. • For a file to be decrypted a key need to be communicated and any key management procedures need to ensure that the source of the key is trustworthy. • Keys need to be communicated securely and kept confidential • In Prime BPM, AES 256 (Advanced Encryption Standard) encryption is in place for all the identified sensitive data when they are stored at rest. **Encryption methods for data in motion:** The transfer of sensitive data through a secure channel. A secure channel is encrypted network connection. Use TLS 1.2 to secure web-based HTTPS communications.

Control A.10.1.2	Key Management
	Key Management is a general need of encryption which enables selective restriction for certain keys. In Prime BPM, Key Management is governed by the hierarchical key distribution comprising of Data Keys and Master Key. **Managing Electronic Keys** Electronic keys are used to encrypt and decrypt messages or digital signatures on messages sent between one or more parties. The management of the electronic keys is critical if confidentiality, authenticity and integrity are to be preserved. Prime BPM manages the electronic keys, to control both the encryption and decryption of sensitive documents to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements. Keys are communicated by reliable and secure methods and kept confidential. Keys for CEO are with CEO and stored in lock and key. Emergency key management process - For keys with CEO the secondary responsibility is with HR head (Co-Founder). **Managing Key Files for accessing the Azure environment** 1. Given to team leaders 2. Devops creates a key file for specific users on azure server 3. Shared privately (with password protection) with the user through email 4. User will install the key file on local system 5. 2 keys – one to connect to jump host and second from jump host to azure. 6. When user leaves the organization, the system admin deletes the private key for the user on azure server, thereby making the individual public key useless. 7. During the employment tenure the team member has to ensure the protection of the key file.

PHYSICAL AND ENVIRONMENTAL SECURITY

Ref. Control Section: --A11

Control A.11.1	Secure Areas
	Prime BPM shall avoid unauthorized access, damage and interference to Prime BPM premises and information. Critical areas have to be identified where dissemination of sensitive information, processing / execution of sensitive projects / programs have been separated by partitions and additional security is implemented as required.
Control A.11.1.1	Physical Security Perimeter
	Based on the security requirement of the assets and risk assessment the security perimeters have been defined and are reviewed from time to time. Security guards' man the premise 24X7 at the main entry to the building. IT team shall ensure that the Information Assets are protected against unauthorized physical access, damage, and interference.
Control A.11.1.2	Physical Entry Controls
	Prime BPM premises are protected by security guards and wherever required lock and key arrangements to ensure that only authorized personnel are allowed access. Access is to be limited to normal working hours for employees (as defined for their current engagement) with exceptions requiring management's prior approval. Employees are required to wear identification badges provided. All doors which can be used for Entry / Exit points are secured using biometric access control and manual lock & key. Wherever manual control is deployed, key access is given to the authorized person.

	Personal identification cards Identification cards are issued to all Prime BPM employees and the employees are required to visibly display the ID card as a means of physical identification inside company premises. The Administration department has procedures for the use of the identification cards. **CCTV Camera** CCTV cameras are installed and used for monitoring.
Control A.11.1.3	Securing offices, rooms and facilities
	Where required, arrangement will be made to house Project/Program/IT Teams handling sensitive projects/ Programs/Data for clients, in separate secure areas. Access to such areas has been limited to authorized personnel only. The Security team will periodically check the access list to ensure that only appropriate staff has access Camera surveillance is used in certain areas of the building and grounds to broaden security capabilities.
Control A.11.1.4	Protecting against external and environmental threats
	CISO, Admin & HR teams shall ensure to implement measures for protection against the damage from fire, flood and earth quake and explosion. Fire detection and extinguishing systems are in place throughout the building, including wiring closets. Computer room fire extinguisher systems are appropriate for use in areas containing servers, switches, routers, and other electronic equipment. Adequate fire protection methods are implemented which includes provision of fire extinguishers of required kinds for different possible fires, fire alarms, sprinklers and smoke sensors, instruction manuals and displays for protection from fire. Emergency phone numbers such as fire brigade, key security personnel, doctors, and hospitals should be posted in prominent places. All offices should have distinct space and pathways, marked as emergency exits as per the recommendations of statutory or external Fire safety agencies. The routes for exit shall be clearly displayed at such entrances. Access to emergency exit doors should not be restricted in any way i.e., boxes, furniture, etc. should never be stored in corridors or near emergency exit doors. Combustible materials and any other materials that may provide fuel to a fire should be kept to an absolute minimum. Wood pallets, cardboard boxes, paper, oily rags, paint and cleaning fluids are materials that may provide fuel to a fire. Flammable liquids should be stored in approved containers and the containers should be under lock and key in metal cabinets.

	All employees and temporary staff should be trained in the fire safety precautions and must be imparted basic knowledge of escape and safety during fire accidents. Mock-drills should be conducted on a yearly basis.
Control A.11.1.5	Working in secure area
	Based on business and security requirement, secure areas have been made unobtrusive and designed to protect the sensitive and critical information and/or assets being safeguarded. CISO will issues guidelines from time to time for working in these designated secure work areas.
Control A.11.1.6	Delivery and loading areas
	All new equipment landing at the premises shall be redirected to a secure isolated area / room till installation. This room shall be properly secured by lock and key and protected against environmental hazards like sun and rain. The equipment's shall be unpacked and checked for the condition of the equipment's. The Prime BPM's Administration department shall check the equipment's and make note of the equipment details and quantity. An inward entry shall be made in the register.
Control A.11.2	Equipment
Control A.11.2.1	Equipment sitting and protection
	Information processing equipment shall be located in an area unlikely to experience natural disasters, serious accidents like chemical spills, damage from exposure to water, smoke, dust, chemicals, electrical supply interference, etc. or other serious incidents. Smoking, eating, and drinking are prohibited in computer equipment areas.
Control A.11.2.2	Supporting utilities
	IT Team / Admin team shall ensure the following to protect equipment's from failures or disruptions: **Redundant sources of power supply** in case of power failure. IT Team shall also plan, evaluate and make arrangements for deploying uninterrupted power supply systems across the organization to reduce risks of equipment damage because of electric fluctuation or outage. Emergency lighting shall be readily available in case of main power failure. **Backup telecom links** wherever necessary and shall be responsible for maintenance, up-gradation and monitoring of the same. All power and telecommunication equipment's are kept in securely enclosed areas under lock and key. Security personnel shall also monitor these areas. **Air-conditioning** shall be maintained for housed equipment's to ensure the smooth

	cooling and functioning less than 20-24 degree centigrade. **Fire protection** - All important places are fitted with fire alarms and smoke detectors. Fire extinguishers are kept at appropriate locations. Fire exits are provided. Fire drill shall be conducted regularly to check the functionality of fire equipment. User awareness training is provided to all Prime BPM employees.
Control A.11.2.3	Cabling Security
	All electric and telecom cables are being laid underground through internal Conduits. Power and Data cables have been segregated and run through separate conduits.
Control A.11.2.4	Equipment Maintenance
	All equipment's come with 1/2/3 warranty based on the type of component to take care of preventive maintenance, replacement and repair during warranty period of the equipment. IT Team shall recommend preventive service maintenance schedules for all sensitive equipment and CISO shall oversee this activity. At the same time IT Team shall ensure that • Ensure service schedules are adhered to. • Only Authorized Maintenance Staff shall have access to sensitive equipment for preventive maintenance, replacement or repair purpose. • Fault Logs and Maintenance Reports are up-to-date for all servers and critical network and power conditioning equipment. • Prime BPM equipment's that are not in use or standby equipment's are kept safely in the storeroom. This room is secured using lock and key.
Control A.11.2.5	Removal of property
	Equipment's carrying information and software cannot be taken off-site without the written approval from CISO
Control A.11.2.6	Security of equipment and assets off-premises
	The use of any information processing equipment out the Prime BPM premises shall be authorized by CISO. In the eventuality of misuse, the equipment's shall be password protected, which shall not allow access to it. Security checks shall be put while taking out the equipment and it shall be allowed, if required only after the approval of CISO. Financial risk can be handled through Insurance and interruption to work can be minimized by maintaining backup of information.
Control A.11.2.7	Secure Disposal or re-use of equipment
	Before disposing off, all information and software programs shall be removed from existing equipment. All such equipment shall be removed only after necessary approval from CISO on producing an undertaking from SYSTEM ADMINISTRATOR that the storage media is cleaned prior to disposal.

	The disposal methods should be applicable as per the security classification of the asset or the information; Mechanisms for disposal shall be – ➢ Crush the equipment ➢ Do format the hard disk for multiple times ➢ In case of outdated equipment - the data shall be destroyed and the machine is degaussed and given to staff or charitable organizations. The data on equipment shall be destroyed before re-using.
Control A.11.2.8	Unattended User Equipment
	Users shall be responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, by providing password protected screen-savers and by logging out or locking the desktop. Unattended equipment will be protected by access control or handed over to IT and protected in lock and key. Terminal sessions to any network devices shall be terminated after 10 minutes of inactivity. Terminal sessions to servers shall be terminated after 10 minutes of inactivity.
Control A.11.2.9	Clear Desk and Clear Screen Policy
	As per this policy no unattended documents or papers should be lying near user workspace. The users shall shred any such document that is not of any use. Housekeeping shall hand over any unattended papers lying in work area or printer area to the admin department. Staff shall be required to store any secure or sensitive information in a secure storage if it is left unattended for more than an hour. All documents shall be kept in a secure storage provided to the users and key shall not be left unattended in or near the secure storage device. All systems shall have password-protected screensavers activating after 05 minutes of non-use.

OPERATIONS SECURITY

Ref. Control Section: --A12

Control A.12.1	Operational Procedures and Responsibilities
	Prime BPM shall ensure the correct operation of its information processing facilities in a secure manner through documented operating procedures with clear-cut segregation of roles and responsibilities.
Control A.12.1.1.	Documented operating procedures
	Standard Operating Procedures (SOPs) for Prime BPM IT infrastructure facilities have been developed. All staff involved in using, administering the IT infrastructure facilities must comply with the Standard Operating Procedures (SOPs).
Control A.12.1.2	Change Management
	Changes to IT infrastructure shall be controlled through a change control procedure. Every change to Prime BPM Information Resource such as: operating systems, computing hardware, networks, and applications shall be subjected to Change Management Policy and shall follow documented Change Management Procedures.
Control A.12.1.3	Capacity Management

With the demands of business growth, Prime BPM shall strategize capacity planning to ensure availability of the resources with least disruption keeping in consideration the increasing volumes of data, no of users, network traffic, etc. IT Team shall plan the future projections and enhancements based on the business growth forecasts.

Following parameters will be monitored by the IT team:

Environment/ Device/ Equipment	Method	Threshold(s)
Servers 1) Disk space 2) CPU utilization 3) Memory Utilization	Monitored automatically on real time basis using the Azure monitoring service. Alerts are enabled for any deviations to be handled	CPU Util :80% Memory Util: 80% Disk Util :80%
Email facility	Dashboards,	Utilization: 80%
Databases	Ex: PRTG SQL sensors, runtime SQL Queries etc.	Storage utilization: 80% DB tuning
Application performance	Tracked manually whenever any performance issues are reported	As and when required by users

Capacity management will be reviewed by CISO on monthly basis.

Control A.12.1.4	Separation of development, test and operational facilities
	Environment for the projects play a major role in the IT world. Wherever feasible test and production environment are separately maintained.
Control A.12.2	Protection from Malware
	To protect the integrity of software and information from viruses, 'worms, Trojans' and other malicious software, Prime BPM shall ensure that only approved/licensed software's are used.
Control A.12.2.1	Control against Malware
	Users are required to comply with software licenses and prohibiting use of unauthorized

	software, obtaining software files from external sources. Files received from an unknown or distrusted source are checked for virus before use. Electronic mail attachments and file downloads from internet shall be scanned using an approved antivirus software. Virus detection and prevention measures and appropriate user awareness procedures are implemented to contain the virus in the network. Protection shall be based on awareness, change management and system access controls. Antivirus update shall be done on for the active systems through the console.
Control A.12.3	Back up
	Prime BPM shall establish routine procedures for carrying out the agreed back-up policy and strategy. This shall include taking backup copies of data and periodic check on and testing for restoration.
Control A.12.3.1	Information Back Up
	This Policy defines the backup policy for systems with in Prime BPM, which are expected to have their data backed up. Refer: Backup and Restoration Policy
Control A.12.4	Logging and Monitoring to record events and generate evidence
Control A.12.4.1	Event logging
	All server storage and critical systems shall be configured to log activities. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows: • All security related logs will be kept online for a minimum of 1 week. • Backup logs will be retained for at least 1 week. • Firewall logs shall be preserved for a period of 1 month and shall be available for reference on site for checking of the logs in case of review. Security-related events will be reported to System Administrator, who will review logs and report incidents to CISO. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to: • Evidence of unauthorized access to privileged accounts • Anomalous occurrences that are not related to specific applications on the host. • Changes to system configuration

	• Auditing of events on critical Windows systems such as successful logons, unsuccessful logons • Privilege modifications
Control A.12.4.2	Protection of log information
	IT Team to ensure logging facility and log information are well protected against tampering and unauthorized access.
Control A.12.4.3	Administrator and operator logs
	Operations performed on the Server storage shall be logged for reference. Enterprise Network storage (File Server) / applications shall be monitored for availability and performance. Discrepancies in performance / errors shall be rectified and logged for analysis and corrective action. Logs shall be independently verified for security breaches & hardware / software alerts.
Control A.12.4.4	Clock synchronization
	Prime BPM shall synchronize all systems and network devices with a Timeserver. This Time server is configured to sync with internationally used Timeservers. This helps to validate all logs and events with accurate time stamps.
Control A.12.5	Control of Operational software
	Objective: To ensure the integrity of operational systems.
Control 12.5.1	Installation of software on operational systems
	IT department performs the installation of all software and applications based on requests and approvals.
Control A.12.6	Technical Vulnerability Management
	Prime BPM shall implement a management process to reduce the risks resulting from technical vulnerabilities.
Control A.12.6.1	Management of technical vulnerabilities

	System Administrator to implement an effective technical vulnerability management in order to minimize risks resulting from exploitation of published technical vulnerabilities. System Administrator to ensure that timely information about technical vulnerabilities of information systems being used is obtained and organization's exposure to such vulnerabilities evaluated and relevant measures taken to mitigate the associated risks, which could include risk assessment, patching, asset tracking and reconnaissance of the organization. Bi-annual or whenever there are any major changes in the applications an audit of the technical vulnerabilities is carried out by approved third parties to keep Prime BPM abreast of the security breaches and published technical vulnerabilities. All high and medium impact findings arising out of these audits will be tracked to closure. Refer: Patch Management Policy
Control A.12.6.2	Restriction of software installation
	Access to software installation is restricted only to the System Administrator, who also maintains a list of approved software's. A request has to be raised in email for any new software installation, which gets serviced only after the approval of System Administrator. Prime BPM uses only evaluated systems and software which are of high integrity. Modifications to software packages are done only in the case of dire necessity. Such changes shall be strictly controlled (Approved by System Administrator).
Control A.12.7	Information systems audit considerations
	Prime BPM shall minimize interference to /from the IS audit process to maximize its effectiveness.
Control A.12.7.1	Information System audit controls
	Prime BPM shall put controls to safeguard operational systems and use audit tools during system audits to maximize the effectiveness. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes. The following shall be observed. ➢ Audit requirements shall be agreed with management. ➢ The scope of the checks shall be agreed and controlled. ➢ The checks shall be limited to read-only access to software and data. ➢ Access other than read-only shall only be allowed for isolated copies of system files, which shall be erased when the audit is completed.

	➢ Requirements for special or additional processing shall be identified and agreed. ➢ All access shall be monitored and logged to produce a reference trail. ➢ All procedures, requirements and responsibilities shall be documented. Refer: Internal Audit Process

COMMUNICATIONS SECURITY

Ref. Control Section: --A13

Control A.13.1	Network Security Management
	Prime BPM shall ensure the secure management of networks through proper network controls and protection of its supporting infrastructure.
Control A.13.1.1.	Network Controls
	System Administrator shall monitor systems of network management. Access to information available through the Prime BPM network systems must be strictly controlled in accordance with approved access control criteria, which is to be maintained and updated regularly. The network shall have been designed to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions. Suitably qualified staff shall manage the Prime BPM network, and preserve its integrity in collaboration with the nominated individual system owners. All Workstations shall be configured for a unique identity before connecting to the Local Area Network. Access to the LAN is provided as per the

	Access Control Policy. Internet traffic shall flow only through the content filtering tool. Authorized traffic from the firewall is, defined on the content filtering security policy, is allowed to pass. The default firewall policies shall be configured to implicitly deny all traffic. The IPS extends the security capabilities of firewalls by providing real time scanning of incoming and outgoing network traffic. Clocks of information systems shall synchronized for accurate recording of instances.
Control A.13.1.2	Security of network services
	Prime BPM uses a combination of Firewalls and Intrusion prevention tools to safeguard and monitor its information assets. All points of entries to the Internet are protected by Firewall. Refer: Network Security Process
Control A.13.1.3	**Segregation in networks**
	Currently Prime BPM setup doesn't demand for an architecture, which shall facilitate in true concept the network segregation. No VLANs have been configured as such, but external networks like internet and applications on parent company have been segregated.
Control A.13.2	Information transfer
	To prevent loss, modification or misuse of information exchanged within Prime BPM and also with any external organizations, procedures and standards shall be established that is in compliance with relevant legislation. This will allow protecting information and media in transit.
Control A.13.2.1	Information transfer policies and procedures
	All computer hardware, software and any data storage medium (for example, hard drives, floppy disks, CD-ROM, USB etc.) and all other modes of electronic communication including the voice mail system in Prime BPM are the property of the Prime BPM. Prime BPM has a legitimate business interest in the proper utilization of its property. Therefore, any use of Prime BPM property, and any communication sent or received via electronic mail, the Internet, the intranet, voice mail or otherwise, may be monitored or reviewed by persons authorized by the Company, at any time with or without notice to employees. Access passwords shall provide certain degree of security; however, it does not guarantee complete privacy and passwords are strictly confidential to avoid misuse of Login Ids.

	Information and software shall be exchanged electronically via e-mail, external links to clients & business associates, information networks and Internet as per the email and communication policy established by Prime BPM. E-mail, voice mail, computer files or any other communication means shall not be used to send personal information, including any obscene information or discuss private matters about anyone, including the self. Any defamatory, insulting or derogatory remark about any person or group of persons via any of these communication channels shall be considered as prohibited. Any employee found, who violates this policy shall be subjected to disciplinary action, including termination.
Control A.13.2.2	Agreements on Information transfer
	Prime BPM shall establish procedures for the exchange of information with 3rd party prior to sending information to third parties and the procedures and Information Security measures adopted by the third party, shall be seen to assure the confidentiality, integrity of the information and non-repudiation.
Control A.13.2.3	Electronic Messaging
	Electronic Messaging Device (EMD) includes Personal computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards, Internet services, mobile data/digital terminals, and facsimile transmissions. • EMD's are designed and intended for conducting business of Prime BPM and are restricted to that purpose. • Transmission of electronic messages and information on communications media shall be treated with the same degree of propriety and professionalism as official written correspondence. • Prime BPM encourages authorized and trained personnel with access to EMD's to utilize these devices whenever appropriate. However, use of any of these devices is a privilege that is subject to revocation based on breaches of this policy. • Employees are advised that they do not maintain any right to privacy in EMD equipment or its contents. Prime BPM reserves the right to access any information contained on EMD's and may require employees to provide passwords to files that have been encrypted or password protected. • Personally, owned EMD's that are used by on-duty employees must be approved by CISO. If used on-duty and the EMD are connected to any Prime BPM network, the personally owned device is subject to the same

	restrictions and guidelines. • Confidential, proprietary or sensitive information may be disseminated only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. • No employee shall access any file or database unless they have a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source. • Unless authorized by the SYSTEM ADMINISTRATOR, employees shall not install any file, software, or other materials without System Administrator approval. • Employees shall not download any executable file, software or other materials from the Internet or other external sources other without CISO's approval. If any employee is uncertain whether or not a file is executable, they should contact the System Administrator for guidance. • Employees shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized. • Employees shall observe copyright restrictions of any documents sent through or stored on electronic mail
Control A.13.2.4	Confidentiality or Non-Disclosure Agreements
	For the protection of information, Prime BPM as an organization has established Security Policy to ensure that all Prime BPM Users become responsible enough to handle security incidences, alert any breach to concerned Security personnel CISO responsible and maintain professional Code of Ethics, including responsibility for confidential information. The CISO will ensure that appropriate Confidentiality and Non-Disclosure Agreement is signed and understood by the users before allowing access to the Prime BPM IT Infrastructure.

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Ref. Control Section: --A14

Control A.14.1	To ensure that information security is an integral part of information systems across the entire lifecycle.
Control A.14.1.1	Security requirement analysis and specification
	Mostly the requirements defined for system by Prime BPM shall be frequently Limited to their internal functions. This requirement includes access to system function or to data and recoverability. Risk assessment and Risk management shall be used as the framework for analyzing security. Security requirements are captured as a part of the Security Requirement Document (SRD) and are also considered during the requirements gathering phase for major new feature.
Control A.14.1.2	Securing applications services on public networks
	All the applications developed are either through SSO (Single Sign On) authentication or form based authentication methods. Modules will be accessed based on the roles assigned to ensure proper authorization. This information will be covered in the security requirement document or Impact analysis during any change implementation
Control A.14.1.3	Protecting application services transactions
	Currently this is not applicable
Control A.14.2	Security in development and support processes
Control A.14.2.1	Secure development policy
	The security requirements will be documented in the requirement / impact analysis documents. Refer: Software Development Process
Control A.14.2.2	Change control procedures
	A formal change control procedure is put in place to control the changes in the Applications. Refer: Application Change Management Policy
Control A.14.2.3	Technical review of applications after operating system changes
	On a bi-annual or whenever there are any major changes in the applications an audit of the technical vulnerabilities is carried out by approved third parties to keep Prime BPM abreast of the security breaches and published technical vulnerabilities. All medium and above impact findings arising out of these audits will be tracked to closure.
Control A.14.2.4	Restrictions on changes to software packages

	Modifications to software packages are done only in the case of dire necessity. Such changes shall be strictly controlled (Approved) and will follow the change management policy Refer: Change Management Policy
Control A.14.2.5	Secure system engineering principles
	Prime BPM shall use the secure information system engineering procedures based on security engineering principles for developing the applications. Data security for the application will be handled as part of encrypting the critical data. Data will be encrypted using AES encryption principle. For the critical applications hosted on public IP, https authentication using the SSL certificate will be deployed. The VAPT testing will be performed for the critical applications hosted on public IP.
Control A.14.2.6	Secure development environment
	Prime BPM protects the secure development environments for its systems development and integration efforts to cover the entire system development lifecycle. Development, test and production environments are segregated and access controls are implemented on the same.
Control A.14.2.7	Outsourced development
	Prime BPM supervises and monitor the activity of outsourced system development. This is done by following: 1. Establishing contracts with the outsourced developer. The terms of contract include: • Retaining code ownership and intellectual property rights related to the outsourced Content • requirements for secure design, coding and testing practices • acceptance testing for the quality and accuracy of the deliverables • Non-disclosure of information 2 Conducting technical vulnerability assessments on the product delivered.
Control A.14.2.8	System security testing
	Prime BPM shall ensure that the developed applications are tested addressing the User roles and access provided based on the application requirement. Refer: Software Development Process
Control A.14.2.9	System acceptance testing
	Prime BPM has established a process to accept new systems, applications or upgrades into production use after appropriate security testing has been performed. Test results of the same are being maintained.
Control A.14.3	Test data
Control A.14.3.1	Protection of system test data
	Prime BPM has established a process for appropriate selection and protection of test data. It is ensured that as far as possible, live data containing confidential information will not be selected and/or masked for testing purpose.

SUPPLIER RELATIONSHIP

Ref. Control Section: --A15

Control A.15.1	Security in Supplier relationships
	Prime BPM has put all the necessary documentation identifying the risks and the security measures that shall be applied to information and information processing facilities being accessed by external party, in event of any breach or security incident. CISO ensures that risks to the organization's information and information processing facility is identified and will deploy appropriate control measures before granting access. CISO has put procedures to ensure external party understands the implications of security incidents and impact of the potential damages.
Control A.15.1.1	Information security policy for supplier relationships
	All departments in Prime BPM should ensure that third parties adequately secure the information and technology resources that they access, process and manage. This includes the information sharing and ensuring non-disclosure agreements are executed to protect confidential information ➢ To protect organizational information or information processing facilities, access control policy has been put in place to ensure that the Security guidelines are being followed by all customers/third parties dealing with Prime BPM, on a regular basis and comply with Information security policy of Prime BPM. As a part of Security guidelines, Prime BPM has clearly outlined the arrangements for reporting, notification and information security incidents, security breaches and also the respective liabilities of Prime BPM and external party. ➢ Access controls such as permitted user ID's, Access controls and user privileges are strictly used as per guidelines and communicated before commencement of work.
Control A.15.1.2	Addressing security within supplier agreements
	➢ Prime BPM as an organization has signed Service agreements with all outsourced party / Service vendors, wherever required service agreement are taken in stamp paper with whom Prime BPM work and have liaison. ➢ Non-disclosure agreements have been signed up with third parties where the information about Prime BPM are exchanged, preventing them from revealing any information learned about Prime BPM assets, technology architecture or operational methodology with specific stress on their information security responsibilities and issues including the indemnification for copying and disclosing information.

	➢ Liabilities of either party in relation to the contract are mentioned in all contracts and all contracts have been ratified by the legal department for completeness of legal clauses and compliance.
Control A.15.1.3	ICT Supply chain
	Agreements made with suppliers include requirements to address the information security risks associated with the information and communications technology services and product supply chain. The following things are considered as appropriate to the supplier services: • Formal management and legal approval • Legal entity providing services • ICT Services provided description • Service level agreements for the services provided • Modification process (Change management process) • Continuity assurances that services will be provided by vendor • Level of access provided to ICT vendor • Security requirements specific to ICT • Adherence to company's IS Policy • Non-disclosure guarantees • Confidentiality agreements • Right to access and right to audit
Control A.15.2	Supplier service delivery management
	To ensure the service is delivered as per the agreement signed by Prime BPM and Service provider, CISO shall check the implementation of the agreed clauses in agreements; monitor the supplier with respect to its activities and performance. This may include ➢ Yearly review reports documenting the supplier's performance relative to service level agreements. CISO shall determine whether contractual terms and conditions have been met, and whether any revisions to service-level agreements or other terms are needed. ➢ Evaluate the supplier's ongoing ability to support and enhance the Prime BPM strategic plan and goals. ➢ Meet with contract parties to discuss performance and operational issues. ➢ Maintain documents and records regarding contract compliance, revision, and dispute resolution
Control A.15.2.1	Monitoring and review of supplier services
	Supplier services shall be governed through service level agreements and service levels shall be monitored on a yearly basis. The uptime terms as per the agreed SLA

	shall define the action thereof. Prime BPM shall review the contingency plans and test the procedures to ensure the uptime is guaranteed and competitive strategic advantage is maintained.
Control A.15.2.2	Managing Changes to supplier party services
	Any changes implemented and incorporated by Prime BPM in security policies and procedures, new controls to enhance the protection levels to minimize the security incidents including reassessment of risks, deployment of new technologies and network enhancements, etc shall be communicated and shall be agreed by 3rd party and the service level agreements amended accordingly.

INFORMATION SECURITY INCIDENT MANAGEMENT

Ref. Control Section: --A16

Control A.16.1	Management of information security incidents & improvements
	Formal security incident management shall be put in place by Prime BPM to minimize the damage from incidents and malfunctions. This will include monitoring and learning from reported incidents and communication to relevant sections of the Organization. As part of training, employees and third-party contractors shall also be made aware of definitions of incidents/weaknesses and defined process for dealing with them.
Control A.16.1.1	Responsibilities and procedures
	Information Security incidents must be properly investigated by suitably trained and qualified personnel. Investigation into an Information Security incident shall identify its cause and appraise its impact on systems or data. This will allow taking preventive and corrective actions, thus preventing it to reoccur.
Control A.16.1.2	Reporting Information security events
	Suspected Information Security events shall be reported promptly to the CISO if found critical. Information Security events shall be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This shall only be done by the CISO or persons authorized by CISO in consultation with the Top Management.
Control A.16.1.3	Reporting information Security weakness
	Security weaknesses shall be reported without any delay to the CISO to speed up the identification of damage caused, its containment and restoration, repair and to facilitate the collection of associated evidence and shall be recorded and processed for corrective action. Breaches of confidentiality shall be reported to the CISO as soon as possible. It shall include breaches of confidentiality arising from a breach of an employee's NDA.
Control A.16.1.4	Assessment and decision of information Security events
	All Security events / incidents reported to the CISO will be analysed by CISO team based on the impact and will involve appropriate function/authority to take corrective action.
Control A.16.1.5	Response to information Security incidents

	The response to the Security incidents / events will be given by the CISO within 8 hours of the incident being reported. There are three levels of incident as per their severity; this will be used to guide incident response: high, medium and low. Depending on the impact assigned the timelines for closure of incidents are defined.
Control A.16.1.6	Learning from Information Security incidents
	The CISO must respond rapidly but calmly to all Information Security incidents, liaising and coordinating with colleagues to both gather information and offer advice. The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations.
Control A.16.1.7	Collection of evidence
	Information Security incidents shall be investigated by competent and skilled personnel. During the investigation of Information Security incidents, dual control and the segregation of duties shall be included in procedures to strengthen the integrity of information and data. Staff shall be advised for assistance and collective action, through defined incident checklists, etc., to handle and respond effectively to an Information Security incident. An abnormal high risk from the threat of electronic eavesdropping and / or espionage activities be identified, all employees shall be alerted and reminded of the specific threats and the specific countermeasures to be deployed. Information relating to Information Security incidents will be released by CISO. **Forensic readiness:** Chain of custody and the protection of evidence are paramount to our operations. All personnel have the responsibility of protecting evidence stored or controlled by Prime BPM. <u>Receipt of Digital Evidence</u> Upon taking possession of digital evidence, the CISO / authorized member shall do the following: A. Immediately note the date and time the evidence was received and whom delivered the evidence (e.g., a person's name or UPS, FedEx, etc.). B. Ensure the needed paperwork has been filed or is accompanying the evidence. This would include, at a minimum, a forensic services request form under most circumstances. C. The evidence will be placed under proper seal if not already delivered in that

condition.

D. The evidence will be properly labelled with the unique case number and individual evidence item number.

Evidence Handling

Forensic examiners and incident responders will often have the need to retrieve evidence as part of their investigation. Evidence should only be out of secure evidence storage for only the absolute time necessary to conduct the examination. While not always practical, evidence should not be left out overnight or during weekend hours.

Evidence Audits

The secure evidence storage shall be audited by the CISO at least every six months. The results of the audit shall be documented in a memorandum and saved as evidence of the audit.

Evidence Retention

Evidence seized by CISO will be maintained in accordance with federal laws, rules, regulations, policies, directives, and guidance from a variety of sources. The CISO is responsible for maintaining evidence properly and for coordinating the release, purging, and destruction of evidence. At no time shall evidence be released, destroyed, or removed from evidence control without the approval of the CISO / Management team.

BUSINESS CONTINUITY

Ref. Control Section: --A17

Control A.17.1	Information security aspects of business continuity management
	Prime BPM shall put a business continuity management process in place for counteracting business interruptions and to protect critical business processes from the effects of major failures of information systems or disasters, so as to ensure timely business resumption.
Control A.17.1.1	Planning information security continuity
	Management is to undertake a formal risk assessment in order to determine the requirements for a Business Continuity Plan. The risk assessment methodology shall identify the events that can cause business interruption along with the probability and impact of such interruptions and their consequences for information security. A risk assessment is carried out by designated members in order to determine the requirements for the Business Continuity Plan. The purpose of Business Impact Analysis (BIA) is to understand the impact that could be caused to the organization if the business process under consideration is disrupted and the concerned department is unable to continue with its core processes. It is carried out to develop an understanding of processes, resources required to carry out the processes and recovery time frames for the critical processes. The analysis includes gathering information regarding Prime BPM's business processes and prioritizing them based on impacts (like financial, regulatory or legal, litigation by clients, health and safety, service to internal customers, public image etc) to the organization due to process failure. **Business Continuity Strategy** The objectives of the business continuity strategies are: • To mitigate the possible impacts of an interruption of Prime BPM's business activities. • To suggest facilities in which the Minimum Operating Requirements (MOR), approved by the management in BIA, can be provided. • To meet the Critical Recovery Time (CRT), approved by the management in BIA. Critical Recovery Time is the length of time the company could survive without those resources, and the time in which those resources would have to be available.
Control A.17.1.2	Implementing information security continuity
	Responsibility-The Top Management / CISO assigns responsibility to an individual or

	team who is responsible for developing and implementing the organizations risk management program. While the team is primarily responsible for the organizations risk management program, Department Heads also participate in the Impact Analysis program. **Frequency-**The Risk Assessment and impact analysis is carried out once in **a year** or any specific changes business processes. **Strategy-** The Recovery Strategy adopted is documented and a report is prepared and approval is obtained from management. A final risk assessment summary is presented as part of the Risk Assessment report, which is then used for Business Continuity Planning. In order to gather the required information and to facilitate identification, comparison and prioritization of business processes, one-on-one meetings are conducted with the help of BIA templates. The interviews are conducted with all security coordinators. This is followed by a second round of meetings with Department Heads, for discussing and analysing the pre-filled BIA templates. The survey is designed to collect the following information: • Business Processes • Customers to the Process (External/ Internal) • Critical Recovery Time • Resources for critical processes • Identification of existing alternatives for the resources for critical processes • Process interdependencies • Various impact of process failure The respondents are asked to identify all the business processes within their departments and identify their Critical Recovery Time (CRT) / Recovery Time Objective (RTO) to evaluate the impact on the organization in the event of disruption of the business processes when they are needed the most. The various impacts due to the unavailability of business processes are rated as High, Medium and Low. This information is subsequently ratified with the head of the respective department. A BIA report is made and submitted to management for approval.
Control A.17.1.3	Verify, review and evaluate information security continuity
	The Business Continuity Plan shall be periodically tested to ensure that the management and staff understand how it shall be executed. All staff shall be made aware of the Business Continuity Plan and their respective roles. Business continuity

	plans in conjunction with recovery plans shall be tested regularly to ensure that they are up to date and effective. Such tests shall also ensure that all members of the recovery team and other relevant staff / 3rd party are aware and well communicated of the plans. Refer: Business Continuity Plan
Control A.17.2	Redundancies
Control A.17.2.1	Availability of information processing facilities
	The data backup is taken on a regular basis with every day and every week back up. To an extent feasible and economically justifiable, redundancies are provided for critical network or other equipment's. redundancies required but not feasible are documented in the risk assessment and management's approval on acceptance of the risk.

COMPLIANCE

Ref. Control Section: --A18

Control A.18.1	Information security reviews
Control A.18.1.1	Independent review of Information security
	Prime BPM will conduct review of its security implementation by third party auditors every year or internal auditors independent of the area being audited twice in a year. Review will also be conducted in case of significant changes in the information security implementation. Any changes and enhancements shall be made to the policy after review with the CISO
Control A.18.1.2	Compliance with security policies and standards
	Department Managers shall ensure that all security procedures within their area of responsibilities shall be carried out correctly to achieve compliance with security policy and standard.
Control A.18.1.3	Technical Compliance checking
	The System Administrator shall conduct network and server security compliance inspection. The program shall identify the area and scope to be covered during inspection and the team responsible to conduct the inspection. The inspection shall be carried out only by competent persons authorized to do the same or only under the supervision of such persons.
Control A.18.2	Compliance with Legal and Contractual requirements
	Prime BPM shall establish legal compliances and explicitly define, document to avoid breaches of any law –statutory, regulatory or contractual obligations and shall meet security requirements standards.
Control A.18.2.1	Identification of applicable legislation and contractual requirements
	The applicable legislation which users shall be required to comply with are as shown below: **Australian Superannuation, Australia Workforce Compensation, Australia ASIC, WorkCover (insurance for staff at work), Superannuation (your provident fund), PAYG Withholding (tax submission on part of staff member), General adherence to Employment Standards/Act called FairWork)** **India Information Technology Act, 2000 (amendment 2008), Copyright Act 1957 (as amended by the Copyright Amendment Act 2012), The Patents Act, 1970**
Control A.18.2.2	Intellectual property rights (IPR)
	Intellectual Property rights shall be honoured and protected as per international convention as India is also a party to it. Appropriate procedures shall be implemented to ensure compliance with legislative,

	regulatory and contractual requirements on the use of material in respect of which there shall be intellectual property rights and on the use of proprietary software products. ➢ Acquiring software only through known and reputable sources, to ensure that the copyright is not violated. ➢ Maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them. ➢ maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights ➢ Maintaining proof and evidence of ownership of license, master disks, manuals etc. ➢ Implementing controls to ensure that any maximum number of users permitted is not exceeded. ➢ Carrying out checks that only authorized software and licensed products are installed. ➢ Providing a policy for disposing or transferring software to others ➢ Using appropriate audit tools ➢ Complying with terms and conditions for software and information obtained from public networks. ➢ Not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law. ➢ Not copying in full or in part, books, article, reports or other documents, other than permitted by copyright law.
Control A.18.2.3	Protection of documented Information
	Important records of the organization shall be protected from loss, destruction and falsification. ➢ The procedures for the storage and handling shall be addressed in chapter on Regulatory compliance process. ➢ The inventory of information assets and information processing assets shall be maintained. ➢ The CISO & System Administrator shall ensure that the category of compliance is maintained as a part of the checklist. ➢ The authorized personal shall have access to relevant records and shall give access to the relevant stake holders based on the need.

	➢ The System Administrator / CISO shall ensure that all the master approvals and licenses are kept in a centralized place with a lock and key and also a copy is kept in company lockers. ➢ On a yearly basis, a copy of all the records is kept in bank locker / Fire safe / offsite location as a BCP / DRP measure. ➢ Records are retained based on the Regulatory compliance check list.
Control A.18.2.4	Privacy and protection of personal information
	Data protection legislation normally covers all types of information which shall be either in electronic form or held as manual records. The legislation normally relates to the protection of the rights of individual persons. Internationally, Data Protection has become an important issue. This policy covers its relevance to staff and third parties. Prime BPM intends to fully comply with the requirements of Data Protection legislation in so far as it directly affects the activities of Prime BPM. System Administrator will assess and issue the guidelines as applicable. Prime BPM may collect, process, store, transmit, and disseminate only that private information which is necessary for the proper functioning of its business. When private information is no longer needed, it shall be destroyed by shredding or other approved destruction methods. Destruction of private information resident on computer disks and other magnetic media must be accomplished with an overwriting process (a simple "erase" process is not sufficient). To assure the proper destruction of private and/or confidential paper document, paper shredder shall be used. Private and/or confidential information should not be removed from Prime BPM offices. Permission to take such information off-site may be granted by the respective owners. Signed third party non-disclosure agreements may additionally be required when private information is removed or sent for further processing from Prime BPM offices.
Control A.18.2.5	Regulation of cryptography controls
	Cryptography Control shall be used in compliance with all relevant agreements, laws and regulation. Legal advices shall be sought to ensure compliance with national laws and regulation as well before encrypted information or cryptographic controls are moved to another country.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.