Bridgestone India Private Limited

IT Department

POLICY

IT Security Policy

Table of Contents

Document Change History and Revision Control

The history of modifications and changes to this document are reflected in this section. All changes, updates, revisions, or comments should be documented and reflected in this section.

Approved by:

Date of approval: 10/05/2022

Id	Sections Revised	Description of Revisions	Changed By	Date
1.0	All	Initial Document Creation	Shailesh Mahajan	01/4/22
2.0	All	Update after stakeholders review	Nitin Gaur, Sagar Bhosale	20/4/22
3.0	All	Final review	Sunil Nair	22/4/22
4.0	All	Approval	Prashant Jagetiya	10/5/22

1. Introduction

In alignment with the Bridgestone Global Security Policy (GSP), this document establishes the high-level IT objectives for securing data within Bridgestone India (also referred to as the "BSID") and guarantee data confidentiality, availability and integrity.

The protection of information or data against threats, such as unauthorized access, modification or loss as well as measures necessary to prevent, detect, document and respond to such threats are key elements to manage Information security.

2. Purpose

This policy establishes the specific targets for IT Security management which govern Bridgestone BSID information systems.

The objectives of the BSID IT Security Policy (ITSP) are to:

- Provide the BSID corporate policy baseline and standard for IT security countermeasures and risk management from the viewpoint of the risk prevention and ensures compliance with legal and regulatory requirements;
- Provide guidance to all BSID Users on how to protect Bridgestone information assets in a manner that achieves a balance of cost effectiveness, reasonableness, and an acceptable level of risk; and
- Provide a common basis for developing BSID security standards and effective security management practices throughout the global company.

3. Scope/Applicability

This policy applies to all forms of information including, but not limited to, reports, presentations, spreadsheets, drawings, documents and any other form of information (collectively, the "**Information**") that can be stored on paper or on electronic and computing devices (servers, computers, USB sticks, mobile devices, or on any other IT media), applications, cloud solutions and network resources used to conduct BSID business or to interact with internal networks and business systems, whether owned, leased or managed by BSID or a third party (collectively, the "**IT Resources**"). All employees, contractors, consultants, temporaries, and other workers at BSID and its subsidiaries, including all personnel affiliated with third parties working on BSID IT Resources and using Company Information (collectively, the "**Users**") are responsible to follow the rules and guidelines as described in this policy and always exercise good judgment regarding appropriate use of IT Resources in accordance with policies and standards, local laws and regulation.

The protection of Company Information and IT Resources is everyone's responsibility. Each User must take personal care for the security of the Information they own, provide or work with.

4. Access Control

4.1. Roles and responsibilities for managing access to the Information and IT Resources must be defined.

4.2. The allocation of access rights must be controlled through a formal authorization process and Users must at least obtain approval from their Head of Department when requesting access. Access must not be provisioned until the appropriate approvals are in place.

4.3. Procedures will be maintained for the approval, change and termination of system and Information access rights.

4.4. Access rights for Users will be issued based on their job responsibilities and as authorized by the Data Owner of the Information or IT Resources involved.

4.5. Modification in access rights must be requested when User's role changes and new job responsibilities require different access rights. Previous access rights must be revoked, if required.

4.6. Access to Information and IT Resources will be granted to Users with an identified business need.

4.7. Individual users accounts accessing Information and IT Resources must be authenticated. Authorization and access will follow the principle of “least privilege” and “need-to-know.”

4.8. Records which contain who has approved, the approval date and which access rights were given, must be maintained according to local regulation and internal retention policies.

4.9. Default application and/or guest accounts access must be revoked or disabled where possible.

4.10. Individual user accounts must never be shared.

4.11. Shared accounts are only allowed for specific accounts (service, administrator, system, root, etc.). These accounts must be used on a case-by-case basis and must be documented by the system owner and approved by IT Security.

4.12. User accounts and generic accounts must be unique.

4.13. User accounts and generic accounts must be linked to an active responsible owner.

4.14. Segregation of duties must be ensured so there are no violations with business or technical roles for Users. If segregating access is not possible then mitigating controls must be considered.

4.15. The Human Resources Department shall communicate the last working day of all employees and third-party users to relevant stakeholders to ensure that the access rights of all employees and third-party users to information and information processing facilities is removed upon termination of their employment, contract, or agreement, or adjusted upon change.

4.16. A compliance check to identify segregation of duties violations must be conducted prior to provisioning access.

4.17. Managers must review and approve the access rights granted to their staff or contractors at least annually. The manager must submit any necessary changes to access rights to the appropriate authorities.

4.18. Login banners will be configured to notify Users of acceptable use of the systems and networks. This banner will appear at the initial login to the Bridgestone network or systems that support banners at the time of initial login. These banners should not display system or application identifiers until the log-on process has been successfully completed.

4.19. All remote sessions or interactive sessions to systems must employ a login inactivity timeout function.

4.20. User login events must be logged and monitored. Contents of logs are defined in “logging, monitoring and reporting policy”.

4.21. Passwords for generic accounts must be changed immediately (at least within next business day), whenever a User with knowledge of the password leaves the company.

4.22. Passwords for generic accounts must be changed within 5 business days whenever a User with knowledge of the password changes role within the company.

4.23. Password must be changed immediately (at least within next business day) if there is any suspicion of the account being compromised

4.24. Controls must be set up to identify the existence of any dormant accounts on a half yearly basis. Once identified, these accounts must be deactivated or removed.

4.25. Accounts and access rights for non-employees (such as contractors, vendors and temporary employees) must be created once all ‘pre’ on-boarding requirements are met according to 3rd party vendor policy. These accounts must be configured with an automatic expiration period.

4.26. All accounts (for employees and non-employees) must be disabled immediately after contract termination.

4.27. Special system privileges, such as the ability to manage a system, administer security or examine the files of other users must be restricted to only authorized personnel.

4.28. Privileged user accounts must be strictly limited to those individuals who require such privileges for authorized business purposes.

4.29. Manager and User of privileged accounts must be identified.

4.30. Privileged accounts must be reviewed and re-authorized semi-annually.

4.31. Shared accounts having privileged rights must have the password changed immediately if a User is terminated or change role. The appropriate change control process must be followed for the password change.

4.32. Privileged users must be informed and trained to ensure proper understanding of the security requirements and responsibilities.

4.33. The allocation of privileged access rights should be controlled through a formal authorization process and must not be provisioned until the appropriate approvals are in place.

4.34. Procedures must be established for the expiration and renewal of privileged accounts.

4.35. The account used for privileged access must be different than the regular user account of the User. Regular day-to-day business functions must not be conducted with the privileged account and system administration functions must not be conducted with a regular user account.

4.36. The account used for privileged access must be linked to an active responsible owner.

4.37. Where possible, default administrative IDs such as administrator, admin and or root must not be used and be deactivated. Administrative IDs must be newly created with different names other than the default name. These new IDs must be nominative per user.

4.38. Controls must be put in place to identify and monitor usage of super user accounts by Bridgestone and non-Bridgestone Users. Super user access and login attempts must be logged and monitored.

4.39. The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

4.40. User authentication for IT systems, network, databases, operating systems and IT infrastructure accounts shall be governed by BSID's Password Management policy.

4.41. Business and maintenance activities being carried out within the application shall be logged for review purpose along with the user ID for review purposes.

5. Asset Management

5.1. An approved asset database must be created and maintained to effectively track all IT Assets that support Bridgestone's data and to confirm BSID IT Assets are properly managed and safeguarded.

5.2. The asset database must include at a minimum the name of asset, type of asset, owner, and location.

5.3. Local procedures must be defined to manage effectively IT assets of local IT environment, including defined roles and responsibilities.

5.4. IT assets database must be reviewed on an annual basis to verify IT assets.

5.5. IT assets database must only contain properly licensed and authorized software.

5.6. Users who have Bridgestone owned IT assets in their possession must return these assets upon termination from the Company. IT asset database must be updated accordingly.

5.7. Bridgestone shall ensure that all IT assets purchased are legal and appropriately accounted for. All documentation of ownership shall be appropriately maintained.

5.8. Bridgestone shall ensure that the employees, contractors and third parties follow the guidelines for the acceptable level of use of all IT assets. Assets must be used for business and operational purposes and must be protected from damage due to unauthorized usage.

5.9. All IT assets shall be classified according to the Data Classification policy. All information must be handled according to their classification levels to ensure their security.

5.10. In order to effectively manage the process of deployment, use, and monitoring of IT assets in Bridgestone, systems and procedures shall be developed and implemented to comply with the legal and regulatory requirements of the region in which Bridgestone operates.

5.11. Asset retention requirements shall be identified by authorized personnel to ensure compliance with legal, regulatory and business requirements.

5.12. Movement of IT assets in and out of the company's premises shall be performed in a controlled manner.

5.13. A register of all movements of the IT assets shall be maintained and reviewed periodically.

5.14. The IT asset inventory shall include all information necessary in order to recover from a disaster.

5.15. All incoming assets shall be subject to a preliminary inspection by the authorized personnel prior to acknowledging receipt of the same.

5.16. Formal procedures for the secure disposal of IT assets shall be established. Secure IT asset disposal shall be enforced to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.

5.17. IT assets shall be disposed only on obtaining the approval and authorization from the respective asset owner.

5.18. All third-party hardware (used for testing, standby, temporary hire or any other purpose) shall be subjected to a review and deletion of the company's proprietary information before it is removed from the company's control.

6. Backup and Recovery

6.1. Data backups and archives must be retained for a period of time as defined in the data retention policies and meet any local regulatory requirements.

6.2. Backups for all critical Information and IT Resources should be stored in a remote location, at a sufficient distance to escape any damage from a disaster and not in the same location as the IT Resource being backed up.

6.3. Backup media containing sensitive Information must be transported offsite with appropriate protection following an auditable and verifiable process.

6.4. Adequate policies and procedures must be provided to ensure all critical Information and IT Resources can be recovered following a disaster.

6.5. Scope and frequency of backup must be defined according to the confidentiality, availability and integrity requirements for the system and the data.

6.6. When planning for new IT Resources, capacity for backup must be reviewed and assessed to ensure secure backup and recovery capabilities.

6.7. Backups must be tested on regular basis to validate recovery capabilities and accuracy and completeness of the backup data.

6.8. Backup media must be classified and treated as equivalent to the stored data.

6.9. Access to backup media must be restricted to authorized personnel only.

6.10. Storage media type must be defined based on retention period of backup data and media aging deterioration. Transferring data to a new media must be planned if the validity of the media is shorter than the data which is stored in it.

6.11. Disaster recovery environment must maintain same level of security as production environment.

6.12. All application and operating systems software, data (including databases), application and operating systems configuration information, hardware configuration information (where applicable) and log files / logs from various systems that need to be backed up shall be identified and documented.

6.13. The backup and recovery procedures shall be monitored regularly.

6.14. In addition to the scheduled / periodic backups, backups shall be taken in case any of the following events occurs:

- Configuration change
- Upgrade of an operational system

6.15. Offsite storage requirements for backup media shall be defined.

6.16. All movement of backup media between offsite and onsite locations shall be tracked and recorded. Backup media shall be transported in a secure manner.

6.17. Backup strategy shall need to be aligned with the respective IT continuity plan.

6.18. Backed up data shall be provided for restoration purposes only after receiving the approval.

6.19. A log of recovered data shall be maintained.

6.20. The entire restoration process shall be documented detailing the annual restoration schedule, the test plan, success criteria, the activities carried out as part of the testing and the test results.

6.21. Exceptions identified during the testing process shall be documented and reported. Root cause analysis of the same shall be performed and corrective actions must be taken.

6.22. All backup and restoration activities shall be performed as per the Responsibility Accountability Consulted Informed (RACI) charts for Backup and Recovery process.

6.23. Retention of backup tapes shall be as per requirement of the system.

7. Encryption

7.1. Only standard public encryption methods can be used in order to perform any encryption activity related to the Bridgestone Information or on Bridgestone IT Resources. Personal or non-standard encryption methods cannot be used.

7.2. Consideration must be given to the regulations and national/international restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information.

7.3. Sensitive Information sent outside of the Bridgestone network must be encrypted using a minimum key length of 128-bits.

7.4. The encryptions requirements are dependent on the sensitivity of the data and the location of where the data is being stored or transmitted to.

7.5. Non exhaustive list of protocols for encrypting data at transit include TLS and SSL for web browsing; SFTP for file transfer; IPSec and SSL VPN for Virtual Private Networks; and Pretty Good Privacy (PGP), OpenPGP, GnuPG, and S/MIME for email, WPA2-PSK for Wireless LAN. When possible, latest version of these protocols are recommended.

7.6. Bridgestone Information can only be hosted with third party vendors who use approved encryption methods for data encryption at rest and in transit. They must have approved key management processes.

7.7. Mobile devices authorized for business use and storing sensitive information must be encrypted.

7.8. Encryption keys are considered as sensitive data and access to those keys must be restricted on a “need-to-know” basis. The keys to be used for encryption must be generated by means that are not reproducible by external parties.

7.9. Keys for highly confidential data or critical infrastructure must have a process for key recovery. Two options for key recovery are a key escrow and the use of a master key. Access to the escrow or the master key must be limited to individuals approved by IT Security team.

7.10. Any production certificate authority managed or used by the Company must have a supporting certificate policy and a certificate practice statement. The certificate authority must operate in accordance to the certificate policy, to the certificate practice statement and applicable laws.

7.11. Registration authorities that operate on behalf of certificate authorities must operate in accordance with its certificate policy and certificate practice statement.

7.12. Root keys for certificate authorities must be protected with physical security, dual control, split key components, and separation of duties.

7.13. The Company preferred standard for public key infrastructure based digital signature protocol is X.509. When using digital signatures, specific conditions under which a digital signature is legally binding must be considered.

7.14. Network communication must be encrypted as stated in network security policies.

7.15. If the confidentiality and integrity of a key can no longer be guaranteed, the key must be revoked and a new key must be created.

7.16. The life-cycle of the key/certification must be defined and managed.

7.17. All data which is Personally Identifiable Information (PII) shall be stored in encrypted format;

7.18. Risk assessment shall be carried out to identify need, methodology and usage of encryption or cryptography.

7.19. Confidential information that is not actively used, when stored or transported in computer-readable storage media (such as servers or USB drives), shall be in encrypted form.

7.20. Where there is a requirement to transfer data to a storage medium, the information shall be encrypted using proven encryption algorithms before the data transfer.

7.21. Information used to verify the identification of remote terminals shall be appropriately protected.

7.22. Static or reusable authentication information shall be encrypted during storage and while passing through the network using encryption software or hardware.

7.23. A secure process for key management should be established and implemented.

7.24. The cryptographic keys shall be protected against unauthorized modification, substitution, unintended destruction and loss. The secret keys associated with symmetric cryptographic algorithms shall be protected against unauthorized disclosure.

7.25. Type and strength of the encryption algorithm to be used in a given situation shall be based on the criticality of the business information handled.

7.26. The length of the cryptographic keys shall comply with contractual requirements and other regulations.

7.27. Encryption keys shall be protected using proven encryption algorithm with higher key lengths.

7.28. Where possible, encryption keys shall not be transmitted over the network. If the keys used to govern the encryption process are to be transmitted over the network, then they shall be transmitted through secure communication channels.

7.29. Process to deal with protection of cryptographic keys in the case of lost or compromised keys should be established.

7.30.

8. EndPoint Security

8.1. All Bridgestone production and non-production servers and Endpoint Devices must have endpoint security software installed, consisting of a minimum of anti-virus, anti-malware and advance capability to manage threats .

8.2. The endpoint security software must be configured to automatically scan files, detect and block malicious code and activity.

8.3. Endpoint protection software should be implemented to scan Bridgestone servers and Endpoint Devices on a routine basis. Scanning should include files received over networks, USB sticks, email attachments, internet downloads and web pages. Any virus found must be cleaned from the machine.

8.4. Signatures, threat information or other related files for endpoint security software must be kept current. If the update process is not automated, a procedure should be developed to regularly monitor, evaluate and update the endpoint security software.

8.5. Endpoint security software must use a centrally managed solution.

8.6. All endpoint security software installed on the servers or on Endpoint Devices must not be removed.

8.7. The network architecture should require proper segmentation and firewall protection between Endpoint Devices and production servers to avoid the internal propagation of malware.

8.8. Environment where propagation of a virus or malware can have operational impacts must be isolated from the rest of the network.

8.9. Unauthorized software are prohibited from being installed on all Bridgestone production and non-production servers and Endpoint Devices. Procedures or controls should be put in place to prevent or detect the use of unauthorized software.

8.10. USB ports must be blocked on all endpoint devices. In case users require USB access to be enabled on their device then it must follow the exception management process.

9. Security Assessment

9.1. Internal Information security assessment must be conducted at least every 2 years to ensure any IT Resource, which is used to conduct Company business, complies with all security requirements regulated by BSID security policies, laws and regulations.

9.2. External Information security assessment must be conducted at least every 2 years by an approved audit partner to ensure any IT Resource, which is used to conduct Company business, complies with all security requirements regulated by BSID security policies, laws and regulations.

9.3. Security assessments must be performed when major changes to infrastructure and applications occur or when new solutions are implemented, to identify any potential risks to the confidentiality, integrity, availability or privacy of the concerned Information or IT Resources.

9.4. Scope and cycle of the security assessment must be defined by IT department.

9.5. The Security assessment must be conducted by an appropriate party in order to respect the segregation of duties.

9.6. Results of security assessments must be recorded and retained for future reference and available to authorized personnel.

9.7. When security assessments are conducted, relevant parties must be informed to ensure proper coordination and collection of information.

9.8. If any major deficiency is discovered during an assessment that would result in a compromise, it must be reported and planned for remediation. Reporting procedures and remediation plans must be defined at the local level.

9.9. Major deficiencies must be retested after remediation.

9.10. Host discovery must be completed twice a year to identify new and unauthorized devices and assess compliance with security requirements.

9.11. Third party security must be assessed to ensure third party compliance to BSID security requirements.

10.Security Awareness

10.1. Security awareness and training program must be reviewed and approved annually.

10.2. Security awareness and training program must be relevant and current to existing environments and IT Resources.

10.3. Users who transfer to new positions or roles with substantially different Information security requirements must receive security training specific to their new assignment before the roles becomes active.

10.4. Mandatory security awareness and training must be measured for completion.

10.5. A security awareness and training program at a minimum must include:

- Required training (on annual basis);
- Training for information sharing only (provided on an adhoc basis);
- Regular communication about general security topics / concerns (provided on an adhoc basis);
- Security exercise drills (on an annual basis);
- Additional definition of the security awareness and training program can be done locally, based on locals specifics and given to all local Users.

10.6. Security awareness and training program must include how to properly identify and report security related incidents.

10.7. Security awareness and training program must include a reference to the security policies and where the documents are located.

10.8. Additional training for safeguarding and securing special or privileged access to IT Resources or Information will be given to the personnel who require that level of access.

10.9. Any relevant security requirements upon leaving the organization must be reminded during the off-boarding of Users.

10.10. Security incident response exercises and training must be conducted annually within the security team and any additional stakeholders who are requested by security team.

10.11. All security policies and documents must be available on company portal/intranet to access for all employees and could be used as reference

11.Logging, Monitoring, Reporting

11.1. Access to Bridgestone sensitive IT Resources or Information assets must be logged to record events or security incidents that are considered relevant.

11.2. IT Resources must be monitored and logged to record events or incidents that have an impact on the availability of the Information.

11.3. Access to logs and log configurations must be authorized, approved and managed.

11.4. All recorded logs must be maintained at a minimum of one year.

11.5. System audit logs and perimeter security devices (or their condensed reports) must be retained for a sufficient period, no less than one year, to permit and support any investigations of events or incidents and comply with all local regulatory and legal requirements.

11.6. Date and time on all systems and devices must be automatically and regularly synchronized to a single reference time source.

11.7. All relevant security event and incidents logs must be monitored daily.

11.8. IDS and IPS systems must be configured to monitor at least all traffic with destinations on the perimeter including all internet gateway, remote access gateways and extranet gateways, points of ingress/egress of major business locations/networks and all traffic inside the DMZ(s).

11.9. All logs must be saved on appropriate devices to ensure compliance with retention requirements and to ensure monitoring capacity of the log file to protect against failure to record events or overwriting events.

11.10. Procedures and processes for incident handling must be defined when detected from security logs.

11.11. Users should be made aware of the procedure for reporting security events and the point of contact to which the events should be reported to.

11.12. Logs shall be monitored and analyzed for any possible unauthorized use of information systems.

11.13. The Company shall inform users of monitoring activities and obtain their consent to such activity.

11.14. Log information shall be protected against unauthorized access, alterations and operational problems.

11.15. Fault logging shall be enabled, analyzed, and appropriate actions shall be taken.

12.Mobile Security

12.1. Policy and procedure must be defined to allocate Mobile devices to access Bridgestone IT Resources and Information.

12.2. Any Users using Mobile devices to access Bridgestone IT Resources and Information must read, acknowledge and sign an end user agreement stating the Bridgestone minimum rights of logging, auditing and wiping the mobile devices in compliance with the local regulations.

12.3. Mobile devices must use an approved secured connection to connect to Bridgestone corporate network and IT Resources.

12.4. “Jailbroken” or “rooted” devices are forbidden Mobile devices to connect to or to access Bridgestone IT Resources and Information.

12.5. Operating systems on Mobile devices must be maintained and kept up-to-date.

12.6. Upon termination of employment, Bridgestone Information must not be copied or stored on Mobile devices and all Bridgestone data must be wiped, including any backups containing Bridgestone Information.

12.7. Mobile devices will be fully wiped in the following circumstances:

- Any devices that is reported lost or stolen will be fully wiped;
- If there is any suspicion that a device has been compromised and there is no alternative remediation, the device will be fully wiped;
- In the event of a separation from the company, corporate owned devices must be returned and will be wiped.

12.8. Audit logs of Mobile device activity and access will be maintained in compliance with logging security requirements.

12.9. Encryption methods that are consistent with the encryption and data classification security requirements, will be used to protect sensitive data that resides on Mobile devices.

12.10. Mobile devices are required to use an approved method for passcoding when accessing Bridgestone IT Resources and Information.

12.11. Passwords or swipe patterns must be managed according to the password security requirements.

12.12. Mobile devices must be configured to automatically lock screen after a defined period, as stated in the security requirements.

12.13. Mobile devices must be configured to lock out after 10 failed login attempts.

12.14. Any lost or stolen Mobile devices must be reported to the Company upon discovery of the missing device. Procedure to report lost or stolen Mobile devices must be communicated to every User.

12.15. Mobile devices authorized for business use and storing sensitive information must be encrypted using authorized encryption methods.

12.16. Mobile devices must be physically protected against theft especially when left in cars and other forms of transport, hotel rooms, conference centers and meeting places.

12.17. Mobile devices carrying sensitive Information must not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure devices.

12.18. Training must be arranged for Users using Mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented.

12.19. If privately owned Mobile devices are used for business purposes, the following security measures must be considered:

- Separation of private and business use of the devices, including using software to support such separation and protect business Information on a private device; if such separation and protection are not possible, then the storing of sensitive Information is not allowed;
- Providing access to business Information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy (local) legislation.

13.Network Security

13.1. Access to any Bridgestone Corporate Network is restricted based upon a documented business need and only authorized users are allowed to access to the Corporate Network.

13.2. Only approved network services and protocols are allowed on the Corporate Network.

13.3. Network communications with Company external destinations must be monitored and logged. These communications must be limited only to authorized destinations.

13.4. Network access control must be put in place to deny access through a security gateway to destinations related to:

- Pornographic/Nudity/Adult content
- Illegal activities/harassment/disparaging of others
- Malicious sites which security vendors indicate as high risk

13.5. Electronic mail and other messaging applications exchanging information through the public network (Internet) must be approved. Access to these solutions must be restricted to authorized IT Resources.

13.6. Access to Bridgestone Corporate Network must be restricted by appropriate network access control systems and granted only to authorized IT Resources or Users.

13.7. Extension of Corporate Network must be granted through an approval process. Approver of network extension permission must be a network owner or a person who is delegated by a network owner.

13.8. Network diagram and documentation must be created for network communications and reviewed at least on a yearly basis.

13.9. Network service manager must be assigned for any part of the Bridgestone Corporate Network. Network Service manager will be responsible to manage the network. Appointment, change and withdrawal of a network service manager must be informed to IT security.

13.10. Bridgestone IT Resources to be accessed directly from the public Internet must be located in a semi-trusted (DMZ) infrastructure.

13.11. IT Resources located in Bridgestone Corporate Network accessing the public Internet must go through a security gateway.

13.12. Any new network devices or solutions to be implemented on the Corporate Network must be approved by network service manager and checked for security requirements prior to implementation.

13.13. DMZ infrastructure design must be approved by network service manager and IT Security. Any IT Resource in DMZ must have an assigned owner. The assigned owner must review and confirm the IT Resource at least annually. Access control configuration of the DMZ systems must be approved and reviewed annually.

13.14. IP address management must be ensured to properly identify location and device in case of identification need.

13.15. It must be possible to identify devices or systems from their IP address or IP range in case of security incident.

13.16. Wireless communication must be encrypted using approved encryption methods and architecture of corporate Wireless LAN must be approved by network service manager.

13.17. Authentication using minimum ID and password is mandatory to access network devices as a privileged user. Default ID and password for privileged account of any network devices cannot not be used.

13.18. Every network device in the corporate network must be identified and under the management of a network service responsible. Privilege access to network devices must be assigned to authorized users. Any changes on network devices must be reviewed and approved prior to implementation.

13.19. The latest signatures, pattern files and threat information of the security filtering or scanning systems must be updated on a regular basis, if possible through an automatic process.

13.20. Communication with public internet web sites must be scanned and monitored by the following security functions and blocked if malicious contents was detected.

- Anti-virus, anti-malware
- Intrusion prevention system (IPS)
- Sandboxing technology

13.21. Network must be segregated into domains. Each network domain must be segregated through network access control system to ensure adequate data protection and limitation of security incident propagation.

13.22. Guest wireless LAN must be completely segregated from the Bridgestone Corporate Network. No access is permitted between those 2 networks. Architecture of Guest Wireless LAN must be approved by network service manager.

13.23. Access to the Guest wireless LAN must be protected and internet access must be filtered and scanned.

13.24. The network domains in which confidential S1 data are stored, must be separated from other network and must be limited to minimum access requirement using network access control systems.

13.25. IP address range of the internal Bridgestone corporate network must not be disclosed to the Internet.

13.26. Connection between DMZ and the public internet must be restricted to approved protocols and filtered through network access control systems. All unnecessary ports or protocols must be blocked by default. New connection request on the network access control system must be documented and approved by IT security. These connections must be limited to minimum IP address and port pair. Communication channels must be encrypted when possible.

13.27. Remote connection to Bridgestone Corporate Network from the public internet must be completed through dedicated remote access gateway. The gateway must be located in DMZ and architecture must be approved by IT security.

13.28. Remote access Users must be authenticated through multi-factor authentication. Remote connections must be encrypted using approved encryption methods. All remote access requests must be monitored and logged.

13.29. Network connections for 3rd party must be completed through dedicated VPN gateway. The gateway must be located in DMZ and architecture must be approved by network service manager.

13.30. Third party VPN connections must be encrypted using approved encryption methods and they must be monitored and logged. Third party VPN connection must be restricted to approved protocols, all unnecessary ports or protocols must be blocked by default. All connections must be limited to minimum IP address and port pair.

13.31. The Bridgestone Corporate Network must be separated in different network domains (physically and/or virtually). Domains must be set up based on trust-levels and/or organizational units. The perimeter of each domain should be defined.

13.32. Electronic mail (email) must be monitored through the following security functions:

- Anti-virus, anti-malware
- Anti-Spam
- IPS
- Sandboxing technology for attachments and URL links
- If malicious content is detected, the mail must be blocked.

13.33. IT Resources that require a higher level of protection or network areas where a higher risk is identified must be segregated into separate physical and/or logical network domains . The interconnection between those network domains must be controlled by network access control devices.

13.34. For IT Resources directly connected to an external or public network (like internet), connection to the management interface will be possible only by a physical connection (console port) or by IP if an access-list is applied on the management interface allowing only authorized devices through an encrypted channel.

13.35. Any incoming traffic from public internet zone to internal Corporate Network is forbidden. Incoming traffic must always go through the semi-trusted DMZ infrastructure.

13.36. The network control access list must be audited and reviewed on a yearly basis.

13.37. Periodic wireless network vulnerability analysis must be conducted to identify rogue access points and devices connected to the network.

13.38. Minimum Baseline Security Standards (MBSS) must be developed and maintained and all network equipment's must be configured as per MBSS.

13.39. Network vulnerability assessments must be performed on an ongoing basis by competent personnel. The risks identified must be documented in the assessment report

13.40. Assessment reports must be used to create corrective/improvement plans and the same must be tracked to closure.

13.41. Third party independent network assessment must be performed annually in order to provide assurance to the management, customers and stakeholders.

14.Password Management

14.1. All Bridgestone domain users must have a user ID and password that uniquely identifies them.

14.2. Passwords are for individual use and must not be shared.

14.3. Shared accounts must be documented and must have an increased access monitoring.

14.4. Users will not divulge passwords or any other authentication credential details to any other individual. It is forbidden to attempt to elicit the password of another user.

14.5. If a password is disclosed it must be changed as soon as the disclosure is discovered.

14.6. The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

14.7. The following should not be used for password construction: dictionary words, repeating characters, whole or partial user names, numbers in sequence such as "123456", whole or partial user ID, company information (Bridgestone/Firestone/Bandag); identifiable personal data (child or pet names, address, birthdates, whole or partial social security number, etc.).

14.8. Passwords will have a minimum length of 8 characters with the exception of

- 12 for administrative accounts;
- 4 for pin access on mobile devices;
- Biometric scan;
- 4 digit swipe pattern.

14.9. Passwords must contain a minimum of 3 out of 4 of the following:

- Upper Case;
- Lower Case;
- Number;
- Special Character.

14.10. Users must not use passwords that are based on previous passwords as they might be easily deduced. Especially passwords that are part of a sequence involving minor incremental changes.

The following examples of sequences of passwords are prohibited:

- Fox84JAN -> Fox84FEB -> Fox84MAR;
- blue36mooN -> blue37mooN -> blue38mooN;
- Purple_1 -> Purple_2 -> Purple_3.

14.11. Accounts will automatically be locked after ten unsuccessful login attempts.

14.12. Password must be locked automatically after 90 days of account inactivity.

14.13. Users must immediately change the default passwords of any newly assigned account or when it has been reset, even if the system does not force the user to do so. At a minimum, all user passwords must be changed every 90 days. Technical controls must be enforced where available to force password changes.

14.14. The account credentials (user ID and password) on all Bridgestone IT assets must be changed from the vendor-supplied default prior to or during implementation.

14.15. Developers or programmers are prohibited to embed fixed passwords in programs code.

14.16. All accounts created in development or test environments must be changed or removed before moving into production.

14.17. When a User changes their password, it must not be same as any of the previous 4 passwords. Controls must be used where available to prohibit password re-use of the previous instances.

14.18. Where technically possible, password controls must be set to ensure the new password cannot be changed by the User for a minimum of three days in order to discourage Users from changing their passwords multiple times to set the password back to the originally defined password.

14.19. Users are individually responsible for maintaining the confidentiality of their credentials (user ID/password).

14.20. Only authorized personnel and system administrators are authorized to change or reset passwords if Users are locked out, unless the system is configured for self-service password reset.

14.21. Identity of the User must be formally authenticated before password reset.

14.22. Users who are locked out of an application must notify immediately the appropriate IT authority. Users who suspect that their passwords have been compromised must report the suspected compromise to the Service Desk immediately, and must change or reset all concerned passwords.

14.23. Passwords for individual user accounts are not allowed to be written down. In any cases, they cannot be left in or near a user’s immediate work environment. Any password that a user may need to be kept in hardcopy must be safeguarded and stored in a locked drawer or cabinet.

14.24. Passwords will not be hard-coded in applications, scripts or files.

14.25. Users must avoid to save credentials (username/password pair) on any internet page.

14.26. Passwords can only be stored in password database application approved by IT Security. Stored passwords must be encrypted.

14.27. Authentication devices (tokens, smart cards, USB keys...) must not be stored with the PIN information required to complete authentication.

14.28. Password must be transmitted separately and anonymously from the username. If they are sent together, the transmission must be encrypted.

14.29. Password can never be stored in clear and must always be encrypted.

14.30. Service accounts must be limited to one function in the system or application.

14.31. Service accounts must not be part of the domain admin group.

14.32. Service accounts must be configured to deny local/interactive logon.

14.33. Service account passwords must be changed at least annually.

14.34. All service accounts must be documented and knowledge of the passwords must be limited to only the administrators that have a need to know.

14.35. All users should be advised to not use the same secret authentication information for business and non-business (private) purposes.

15.Physical Security

15.1. Any Bridgestone IT Resources containing data or sensitive Information must be physically secured and protected from unauthorized access, damage, or interference.

15.2. Physical protection must be commensurate with the identified risks and the sensitivity of the Information and IT Resource to be protected.

15.3. Only authorized individuals will have physical access to data centers, IT equipment closets and IT operations centers.

15.4. Access to secure IT locations must be recorded and retained based on defined retention requirements. The logs should be reviewed on a monthly basis, or when suspicious activity has been reported.

15.5. Visitors to data centers and equipment closets must be accompanied by an authorized party authorized by the Company. Sign-in and sign-out logs must be maintained for all visitors.

15.6. Access to secure IT areas that display sensitive information must be restricted to authorized individuals to prevent unauthorized individuals from observing display outputs.

15.7. Secure IT areas or IT datacenters hosting Information or IT Resources must be geographically located and positioned to minimize potential damage due to physical or environmental hazards.

15.8. Security perimeters shall be defined and used to protect areas that contain sensitive Information and IT Resources facilities.

15.9. Physical access entry points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled to avoid unauthorized access. Emergency exits should contain audible or monitored alarms to alert security personnel.

15.10. Equipment, Information or software should not be taken off-site without prior authorization.

15.11. Long-term alternative power supplies (i.e. UPS, Generators) must be implemented in secure IT areas to ensure minimal impact on operations in the event of a power outage.

15.12. Adequate environmental controls (i.e. fire detection and suppression, water leak detection, temp/humidity sensors, etc.) for secure IT areas must be maintained and monitored to ensure availability of IT resources.

15.13. All environmental control equipment for secure IT areas must be maintained and certified as required by applicable local regulations and equipment specifications.

16.Secure Development

16.1. Development teams must define and follow a documented software life cycle.

16.2. During development, environments (prod, test, dev…) must be isolated from each other. Access to these environments must be based on the principle of least privilege and allowed to authorized personnel only.

16.3. Version control must be implemented in the software development lifecycle and all changes must be tracked following local change management controls.

16.4. All new and changed coding must go through unit testing, acceptance testing, security testing and approved peer review.

16.5. Only authorized personnel should have access to the development environment.

16.6. Test data must be secured according to their classification.

16.7. Prior to production deployment, all new applications should have an application security assessment performed. All findings are to be remediated prior to deployment.

16.8. During the development lifecycle positive and negative testing must be performed.

16.9. Applications must be designed to meet the following criteria:

- definition of the required level of confidentiality, integrity and availability and compliance to the appropriate policies according to the level.
- definition and documentation of the requirements for security (e.g. compliance, data handling, authentication, encryption, logging and business continuity).
- protection of the applications and systems from external cyber-attacks and data leakage, preventing vulnerabilities of the application and other related software.
- Program codes must be available only to authorized personnel.
- prevention of data leakage of the code during release process and under production.

16.10. Development platforms must be secured, and have secure coding guidelines for each programming language used.

16.11. Test data must not include confidential data or personal data as defined by local laws and regulations.

16.12. Test data and accounts must be deleted prior to migrating the application to the production environment.

16.13. Protocol and services which are not necessary must be disabled.

16.14. System and applications developed must include the following security requirements for the log-on process :

- A notice to users for authorized use only
- Not provide help messages during the log-on procedure that would aid an unauthorized user
- Not indicate which part of the data is correct or incorrect if error condition arises
- Protection against brute force attempts
- Logging of successful and unsuccessful log-on attempts
- Masking of passwords
- Encryption of passwords while in transit
- Terminated inactive sessions after a defined period of inactivity.

16.15. Where system development is outsourced, licensing arrangements, code ownership and intellectual property rights related to the outsourced content must be contractually defined.

16.16. All activities of outsourced application development must be supervised, monitored and compliant to the security policies and standards.

16.17. Specific approvals shall be required at relevant stages of the system development lifecycle, as documented in the system acquisition, development and maintenance process.

16.18. User Requirements Specifications (URS) document shall be developed capturing the key functional and non-functional requirements of the system, considering the key business, security, performance and scalability needs.

16.19. Functional and non-functional requirements shall be translated into a high-level design specification for system acquisition, implementation and maintenance.

16.20. High level design requirements shall be translated into detailed design specifications, taking into account the organization's technological direction and information architecture, aligned to the technology planning and architecture process. Reassessment of the design shall be conducted when technical or logical discrepancies occur during development or maintenance.

16.21. Software and technology infrastructure QA plans shall be developed, resourced and executed to obtain the quality specified in the requirements definition.

16.22. The status of individual requirements (including all rejected requirements) during the design, development and implementation shall be tracked, and any changes to requirements shall follow the change management process, till the lifecycle of the system development.

16.23. In the event of major changes to existing systems that result in significant change in current design and/or functionality, a process shall follow similar to that of the development of new systems.

16.24. Internal control, security and auditability measures shall be implemented during configuration, integration and maintenance of systems to protect resources and ensure availability and integrity.

16.25. A strategy and plan for testing the system shall be prepared and the criteria for acceptance of the requirements of new systems, upgrades and new versions shall be defined.

16.26. Program source code shall be stored under restriction and only authorized personnel must have access to the same with appropriate code version control mechanism in place.

16.27. System test data shall be selected carefully, protected and controlled.

16.28. Data input to information systems shall be validated to ensure that this data is correct and appropriate.

16.29. Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

16.30. Integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives shall be ensured.

16.31. Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

16.32. Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

16.33. Modifications to software packages shall be discouraged. All necessary modifications (including configuration changes, changes to reports, etc.) to software packages shall be made in a controlled manner with appropriate approvals.

16.34. If the system is developed by a third–party, the following shall be done:

- The system development processes shall be in compliance to all legal and contractual aspects and to the Systems Acquisition, Development and Maintenance Process;
- Appropriate licensing agreements and contractual requirements for quality and accuracy of code shall be obtained;
- Assurance shall be obtained from the third party for quality and accuracy of the work carried out;
- Ownership of the source code shall be with the Company. If this is not feasible to the third party, the code shall be kept under an escrow arrangement;
- Rights of access for audit of the quality and accuracy of the work shall be obtained; and
- Testing processes in accordance with Systems Acquisition, Development and Maintenance Policy shall be developed.

16.35. To enhance the usability and operation of developed systems, training manuals for operations, support and troubleshooting shall be developed.

16.36. Migration and installation of systems in operational environments shall be controlled.

16.37. All proposed system changes shall be authorized and reviewed to verify that they do not compromise the security of either the system or the operating environment, and shall follow the change and release management process.

16.38.

17.Vendor Third Party

17.1. Third parties must acknowledge and adhere to the relevant Bridgestone security policies.

17.2. Approved third party entities will provide to Bridgestone a list of primary and secondary points of contact responsible for the third party organization's operations which shall be maintained and kept current.

Third parties must notify Bridgestone immediately of any applicable changes of contact information.

17.3. Network connections with third parties must be done securely to protect Bridgestone Information and IT Resources. All connections to networks outside of Bridgestone are required to meet all necessary Bridgestone security requirements.

17.4. All access of third parties to Bridgestone Information and IT Resources requires the use of an authenticating mechanism approved by IT Security.

17.5. All initial requests for third-party connectivity or access to Bridgestone data must be reviewed and approved by Bridgestone IT Security prior to allowing access.

17.6. Security requirements and controls in place at third parties must correspond with the risk level of the associated data they manage.

17.7. Multi-factor authentication must be used to authenticate third party remote access to the Bridgestone Corporate Network.

17.8. All requests for third parties to share data or connectivity with Bridgestone Corporate Network or IT Resources are subject to an audit to evaluate the security, controls, and risks.

17.9. Bridgestone reserves the right to audit third parties or review audits about third parties done by approved independent auditors when contracts or agreements with third parties request access to S1 confidential data. Additional proof of industry certifications may be required to ensure adequate protection meets all Bridgestone security requirements.

17.10. Third-party network based services must have information security policies that comply with Bridgestone's security policies and requirements and must be reviewed by Bridgestone IT security and compliance.

17.11. If third parties sharing connectivity to the Bridgestone network detect a suspected security breach or incident, this event or anomaly must be reported to Bridgestone IT Security or service desk immediately, in accordance with the Bridgestone incident response procedures.

17.12. Third parties have a responsibility in their environment to preserve , protect, and maintain all logs of systems, components, and other evidence related to security breach for forensic investigation and analysis. All log records and forensic evidence must be made available to Bridgestone upon request.

17.13. Appropriate actions will be taken against any third party determined to be the cause of a security breach, incident, outage, or event, and may result in immediate termination of the connection/partner agreement with said parties. If warranted, and at the discretion of Bridgestone Management, this may include pursuing legal action, which may include civil, and/or criminal complaints, injunctions, or other actions.

17.14. The approved third party must restrict the activities of its approved personnel, staff, and subcontractors to only the level of access necessary to perform their responsibility or function.

17.15. Third parties are not permitted to perform system administrative functions on Bridgestone equipment without express permission. All system administrative changes must be performed by a Bridgestone authorized administrator and follow the local change management process.

17.16. All Bridgestone owned equipment located at third-party sites is to be used for its intended business purposes as stated in the contractual agreement. Any misuse of access or tampering with Bridgestone provided hardware or software may result in termination of the agreement or contract, and may warrant other legal action.

17.17. Approved third-party network connections are to be used for business purposes only, as specifically defined and limited in the approved third-party request.

17.18. Bridgestone resources may not be used or perform functions for other unapproved parties, organizations, or internal third party operations.

17.19. Third parties must segregate, logically and/or physically, Bridgestone networks, systems, and data from their internal environment to compartmentalize data and systems.

17.20. Third party systems supporting Bridgestone business operations must be backed up and be compliant with the security requirements.

17.21. Procedures must be in place to monitor and control access from third parties to the Bridgestone network.

17.22. All third parties long term consultants are required to follow the Bridgestone security awareness training.

17.23. Third parties agreements should be established and documented to ensure that there is no misunderstanding between Bridgestone and third party regarding both parties' obligations to fulfil relevant information security requirements.

17.24. Monitoring and review of third party services should ensure that the security terms and conditions of the agreements are being adhered to and that security incidents are managed properly.

17.25. Changes to the provision of services by third parties should be managed, taking into account the impact on security of business Information and IT Resources involved including re-assessment of risks.

17.26. All third-party services shall be identified and categorized according to supplier type, significance and criticality.

17.27. The requirements, scope, level of service and communication processes to be provided by the third party(s) shall be documented in Underpinning Contracts (UCs) and agreed by all parties.

17.28. Risks relating to third parties' ability to continue effective service delivery in a secure and efficient manner on a continual basis shall be identified and managed.

17.29. Standard clauses such as confidentiality or non-disclosure, penalty, right to audit should be included in all contracts and service agreements, as applicable.

17.30. A process to monitor service delivery from external parties shall be developed to ensure that the third party is meeting current business requirements and continuing to adhere to the contract agreements and supplier service levels. Actions for improvement identified during this process shall be recorded and input into a plan for improving the associated services to the business.

17.31. Annual reviews of the contracts, formal agreements or UCs shall be carried out to ensure that business needs and contractual obligations are being met.

17.32. A process shall be in place to deal with the expected end of service, early end of the service or transfer of service to another party.

18.Vulnerability Management

18.1. Vulnerabilities will be identified by actively and passively testing through vulnerability scanning, penetration testing, and the monitoring of external sources for threats and vulnerability announcements.

18.2. Penetration Tests must be compliant with local and global regulatory requirements.

18.3. Penetration Tests must be performed on an annual basis with scope validated by IT Security. External penetration tests must be included in the scope of the annual exercise.

18.4. Penetration test must be performed by Bridgestone authorized personnel or authorized third parties.

18.5. Incident response teams and service desk must be involved during penetration tests.

18.6. High and above rated vulnerabilities identified from a scan are to be verified to ensure there are no false positives.

18.7. All vulnerability and penetration scans will be concluded with a report including the scope and scan results.

18.8. As newly announced critical vulnerabilities are discovered, relevant tests will be performed to ensure that potentially affected systems are remediated in a timely manner.

18.9. When the remediation of vulnerability is reported, that remediation must be validated and confirmed through a new scan exercise.

18.10. All identified critical and high rated security patches must be applied and given priority during patching cycles. When requested by the information security team due to high risk vulnerability exposure, remediation needs to be applied immediately.

18.11. The location of IT Resources that are potentially vulnerable to a critical vulnerability must be determined and identified. This location must be physically or virtually segregated from the other zones.

18.12. Patches should be tested and the risk should be evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. If no patch is available or patches are not installed, other remediation controls must be considered.

18.13. The vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency.

18.14. Procedures must be defined to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization should evaluate risks relating to the known vulnerability and define appropriate detection and corrective actions.

18.15. A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities. Once a potential technical vulnerability has been identified, associated risks and the actions to be taken must be identified.

18.16. Roles and responsibilities should be defined and associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required.

18.17. For Bridgestone sponsored development of critical applications, a threat model must be prepared to assess the risks and corresponding mitigations. A threat model includes a high-level data flow model that illustrates every point in which information moves into or out of the application code or between major parts of the code.

18.18. All newly developed and modified applications must undergo at least one source code review exercise after successful user-acceptance testing has been completed.

19.Glossary & Definitions

Policy - Contain high-level statements of management's directives (WHAT) for the approved use of information resources. In that sense, it states WHERE the Company's strategies for information use are headed. A set of generalized statements, policy describes the overarching information protection objectives for the organization. Policy statements are generally accepted practices for achieving internal control, for addressing current and future information protection goals, and are written in a general manner so that they do not require frequent revision. Adherence to policies is mandatory.

Standards - Support the Policy and describe in detail, HOW we should do to comply with the Policy and what are the associated roles and responsibilities (WHO). IT security standards are statements that provide guidance on how to realize the objectives indicated by policies and comply with them. Depending on references to scope, an information security standard may target more specific groups, domains, technologies, or communities, as compared with the target of the information security rule. Standards are also mandatory statements that define how business activities will be performed to protect Bridgestone information.

Guidelines - Discretionary statements which should be followed for best practice.

Data Owner - An entity or user that creates the information data and authorizes or denies access to data. It maintains accuracy, integrity, and timeliness and has ownership of the data.

Endpoint device - Internet-capable computer hardware device on a TCP/IP network. The term can refer to desktop computers, servers, laptops (or tablets with similar capabilities) or thin clients. Smartphones and tablets, printers bar-code scanners or other specialized hardware such POS terminals or smart meters are not considered as endpoint in this policy.

Mobile device – A mobile device is an Internet-capable hardware device like smartphones, handheld devices or tablets. Desktop computers, laptops (or tablets with similar capabilities) or thin clients are considered as Endpoint device.

Corporate Network - group of IT Resources, interconnected together in a building or in a geographical area. This network, providing native access to BSID IT Resources, must be dedicated to Bridgestone Company and must be fully segregated from any public network or any other companies network.

20.Policy Compliance

20.1. Compliance Governance

Each User must comply with the requirements detailed in this policy. The Bridgestone Security Committee is responsible for approving this document. The IT Security team is responsible for issuing, reviewing, managing this document.

20.2. Compliance Measurement

The Company will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

20.3. Exceptions

Situations in which the requirements in the BSID Security Policy cannot be adhered to must be registered as an exception.

Registered exceptions must contain at least the following information:

- Reference to requirement
- Subject
- Unmitigated vulnerability

- Compensating measure(s)
- Expected Duration.

Exceptions must registered in a central Exception Register.

For each exception, a risk assessment must be performed. For identified risks possible compensating controls need to be analyzed and identified.

Compensating controls must be implemented to mitigate the risks that exist as a result of not complying the requirements in the BSID Security Policy.

Any exception to the policy must be approved in advance by the IT Security team.

Registered exceptions must be reviewed yearly to assess if compensating controls still mitigate the risk or if the motivations for accepting the risk are still valid.

20.4. Non-Compliance

User found to have violated this policy may be subject to disciplinary action in accordance with local regulations.

21.References

The IT security policy is based on input from several sources including the global minimum security requirements aligned globally between the Bridgestone SBUs (BSJ, BSAM, BSCAP and BSID) and some "best practice" frameworks, such as the ISO/IEC 27000 standard :

- ISO27001: 2013 Information technology – Security techniques – Information security management systems – Requirements
  http://www.iso27001security.com/html/27001.html

- ISO 27002-2013: Information technology – Security techniques – Code of practice for information security controls
  http://www.iso27001security.com/html/27002.html#StructureAndFormatOfISO17799

For this reason, the principles (and structure) of the BSID IT security policy are based on a balanced approach.

This document supports other BSID's policies, standards and procedures for the protection of confidential Information including:

- Trade Secrets Policy
- Data Classification policy
- Controls for Data Classification policy
- Cloud policy