V2FSOLUTIONS
Technology | Consulting | Outsourcing

9/9/2025

Internal IT Policy

For V2F Solutions

Ali Hassan
V2F SOLUTIONS

Version: 2.0
Original Implementation Date: February 1st, 2024
Last Updated (Revision): August 1st, 2025
Change Summary: Revised and expanded the “Data Backup and Recovery Policy” section.

Table of Contents

Dear All,

I hope this message finds you well. Starting 1st Feb 2024, we are implementing a new Internal IT Policy aimed at enhancing our IT operations.

Please take a moment to review the attached policy document. Your cooperation is vital in ensuring a secure IT environment. If you have questions, contact our IT department.

Kindly acknowledge receipt by emailing back.

Thank you for your prompt attention.

Best regards,

Ali Hassan
GM IT & Marketing

Purpose:

The purpose of this Internal IT Policy for V2F Solutions is to establish guidelines for the appropriate use, security, and management. This policy aims to enhance the productivity and security of our organization.

Scope:

This policy applies to all employees, contractors, and authorized users who utilize IT resources and technology provided or approved by V2F Solutions. It covers all aspects of IT resource usage, including hardware, software, networks, and data.

Acceptable Use Policy:

Our Acceptable Use Policy outlines the guidelines for using V2F Solutions Company's resources. Employees are expected to utilize company-provided IT assets exclusively for work-related purposes. It is imperative to safeguard sensitive data, refraining from sharing, storing, or transmitting company information without proper authorization. Installation of software and hardware must adhere to company-approved standards, and any identified security vulnerabilities should be reported promptly. Employees should exercise caution when using the internet, avoiding non-business websites and downloads, and remaining vigilant against phishing attempts and malicious sites. Social media representation must maintain professionalism, refraining from disclosing confidential information. Official communication should occur through company email, excluding spam, chain letters, and unauthorized distribution. Policy violations or security concerns must be reported promptly to IT support. Non-compliance may lead to disciplinary actions.

Data Security:

Data Security is a top priority, and it requires the active participation of all users. Users play a pivotal role in preserving the integrity and confidentiality of company information. Responsibilities include stringent access control: limiting access to authorized personnel with strong, unique passwords; never sharing login credentials. Encryption is essential for secure data transmission and storage. Users must remain vigilant against phishing attempts, avoiding suspicious links and safeguarding confidential information. Physical security is crucial, ensuring company devices and data are never left unattended or accessible to unauthorized individuals. Proper data classification and immediate incident reporting are also user obligations. Data Security relies on the collective effort of all employees to maintain a robust defense against breaches and data leaks.

Remote Work and VPN Usage:

In our Remote Work and VPN Usage policy, employees accessing company systems remotely must prioritize security. Utilizing a Virtual Private Network (VPN) is mandatory to establish a secure connection, encrypting data transmission. Users are expected to connect only to password-protected networks and maintain updated security software on personal devices. This policy safeguards against unauthorized access, ensuring the confidentiality and integrity of company data. Additionally, remote work guidelines emphasize the importance of secure communication channels and adherence to data privacy protocols. By adhering to these measures, employees contribute to a resilient remote work environment that prioritizes the protection of sensitive information and maintains a robust security posture.

Software and Application Usage:

Adherence to authorized Software and Application Usage guidelines is crucial for operational efficiency and data security. Users are expected to install only approved software as specified by the IT department, refraining from unauthorized applications. Strict compliance with software licensing agreements is mandatory, and any concerns must be promptly reported. Regular updates, especially security patches provided by IT, are vital for enhancing system security. Prohibited or unapproved software installations, including any forgery of MS Office and MS Windows keys, are strictly prohibited, as they may compromise system stability. Users should be aware that software and application usage may be monitored for compliance and security purposes, contributing to a secure and well-managed software environment.

Data Backup and Recovery:

This policy outlines the data backup, archiving, and recovery standards required to protect the information assets of V2F Solutions and its associated entities (e.g., SkySys, Maxcon). These measures are intended to ensure data resilience, business continuity, and compliance.

---

1. General Guidelines

1. All users must ensure **regular and complete backups** of business data to prevent data loss caused by system failure, cyberattacks, human error, or theft.
2. **Backups must be stored offsite**, meaning they are saved to the **designated external HDD physically located in the office but isolated from user systems**. This device is securely managed and is considered our *offsite location* for internal policy purposes.
3. IT should maintain list of all cloud storage solutions and should regularly obtain confirmations from relevant business/function heads that the storage is being done securely and in line with company's policies and guidelines.
4. Backup data must be **periodically verified for integrity** and retrievability by relevant business/function heads and report compliance to IT from time to time.

---

2. Remote Work and Backup Frequency

5. All employees working **remotely**, in **hybrid settings**, or **outside the premises for more than 5 working days** are required to **transfer their local data backups to the office-designated external HDD** at least once every 7 days when they are in the office or via a secure cloud folder assigned to the business or the function.
6. Backup confirmations must be logged or acknowledged via email to IT.

---

3. Department-Specific Backup Practices

Finance and HR

7. Use **official Google Drive accounts** for storing and backing up all critical business files (e.g., financial records & reports, payroll data, employee records, invoices).

8. These Google accounts shall be created by relevant function head and these accounts should be considered property of the company.
9. Each Google ID **must have function head's and CEO's V2F Solutions email address set as the recovery email**, ensuring access continuity.
10. These Google accounts shall be accessible only to the relevant function head and the CEO.
11. Upon resignation or departure of any HR or Finance employee, password of these accounts must be changed and shared with the current function head and the CEO.
12. **Real-time sync** must be enabled using Google Drive Backup & Sync or Drive for Desktop.

Software Development (SD)

12. Uses a dedicated **OneDrive account provided by Skysys** for secure project backups.
13. Must regularly back up:
    1. Source code for all active and archived projects
    2. Custom development deliverables
    3. Customer documentation (SRS, technical specs, user manuals, deployment guides)
    4. Development tools or configs
14. All backups must follow **version control and naming conventions**, such as:
    ClientCode_ProjectName_ModuleName_v1.2_2025-05-01.docx
    Repo_Backup_ProjectName_2025-05-01.zip
15. SD team leads are responsible for defining and enforcing folder structures, e.g.:

CopyEdit

/Clients/

/ClientA/

/Source/

/Documentation/

/Deployables/

TRG (SkySys)

16. As the **Technical Recruitment Group** for SkySys, TRG follows the same OneDrive backup standards as SD.
17. TRG must back up all necessary records which may be needed for access in future, following are shared as an example only:
    1. Candidate profiles
    2. Recruitment analytics or feedback reports

18. Naming conventions and folder structure should clearly segregate client-based submissions and internal records.

Maxcon

19. Treated as a **client of V2F Solutions**.
20. Maxcon's data (e.g., files) must be backed up in a OneDrive on individual IDs.
21. Maxcon may access deliverables via a secure shared OneDrive folder.
22. Maxcon-related work by internal departments must be treated with the same priority as client delivery backups.

---

4. Google Accounts Governance

23. All **official Google accounts** used across departments must be:
    1. Registered under V2F naming conventions.
    2. Have V2F email addresses as recovery emails.
    3. Be verified periodically by the IT department.
24. IT shall maintain an inventory of all official accounts and conduct periodic compliance reviews, especially during staff exits or transfers.

---

5. Compliance and Oversight

25. The IT department is responsible for enforcing this policy across all departments.
26. Regular **audit logs** and **reporting mechanisms** will be maintained.
27. Any non-compliance, data negligence, or policy breach may result in disciplinary action.
28. Training will be provided to all staff annually or as required.

Device Management:

Device Management is vital for maintaining the security and integrity of company IT assets. To adhere to this policy, users are expected to:

1. **IT Hardware Storage:** All IT hardware, including laptops and other devices, must be securely stored in the office when not in use. Permission from the IT department is required for removal. Users need to get approval from line manager and post a form online. You can also email to itdesk@v2foslutions.com.
2. **Car and Trunk Storage:** Users should not store IT equipment in their vehicles. Company-owned devices should never be left in cars or trunks to prevent theft or damage.
3. **Transport Guidelines:** It is prohibited to transport laptops or IT equipment on bikes between home and the office. This measure is in place to safeguard against potential damage and security risks.

Users are responsible for following these guidelines to ensure the safety and security of company devices.

Software Updates and Patch Management:

Integral to system security, Software Updates and Patch Management require users to promptly apply updates, ensuring the deployment of the latest security patches and enhancements. Adherence to patch management protocols is essential, ensuring compliance across all devices and software. Recognizing scheduled maintenance windows is crucial to minimizing disruptions during the updating process. Users are encouraged to report any identified security vulnerabilities promptly to the IT department for swift resolution. Enabling automated update features, where available, streamlines the patch management process, contributing to a secure computing environment and fortifying the overall resilience of the system.

Social Media and Online Behavior:

Maintaining professionalism is paramount in Social Media and Online Behavior. Users are expected to conduct themselves with discretion, portraying a positive image of the company. Strict confidentiality must be observed, refraining from sharing sensitive information. Interactions online should be respectful, avoiding offensive language or actions that could tarnish the company's reputation. It's crucial to separate personal and professional online activities, ensuring personal opinions don't reflect on the company. Adherence to these guidelines fosters a positive online presence, upholds the company's reputation, and contributes to a culture of respect and integrity in the digital realm.

Training and Awareness:

Training and Awareness are pivotal for fostering a secure work environment. Users should actively engage in regular security training sessions to stay informed about evolving cyber threats and best practices. Developing a sharp awareness of phishing risks is crucial, enabling users to recognize and avoid suspicious emails or links. Understanding and adhering to data protection policies is emphasized, especially regarding the safeguarding of sensitive information. Compliance education sessions are integral to ensuring users understand and comply with company policies and industry regulations. Additionally, fostering a culture of awareness encourages prompt reporting of any security incidents or policy violations, contributing to a robust defense against potential risks.

IT Procurement Process:

The IT Procurement Process at V2F is streamlined for efficiency and accountability. All procurement is exclusively handled by the IT department, and those with requirements can email itdesk@v2fsolutions.com. It is mandatory to discuss requirements with the respective line manager before involving procurement. V2F has established registered vendors, and no external purchasing is permitted without written approval from management. This stringent process ensures centralized control, effective communication, and adherence to established vendor relationships, contributing to a transparent and well-managed procurement system.

Bring Your Own Device (BYOD) Policy (if applicable):

Our BYOD Policy combines flexibility with stringent security measures. Employees may use personal devices for work, adhering to company guidelines. Devices must meet security standards, including updated antivirus software. The IT department may install necessary security applications. Users are responsible for data protection and must promptly report security issues. In case of loss or unauthorized access, company data on personal devices may be remotely wiped. Additionally, IT

needs to be informed of incoming devices, including their MAC addresses, ensuring comprehensive network visibility. This policy strikes a balance between convenience and data protection, safeguarding company information and network integrity.

Data Retention and Privacy:

Our Data Retention and Privacy policy define the guidelines for responsible data management. Data must be retained only for necessary periods, balancing operational needs with privacy considerations. Personal information is handled with the utmost confidentiality, adhering to privacy regulations. Employees must categorize and store data appropriately, ensuring compliance with legal requirements. Access to sensitive data is restricted to authorized personnel, safeguarding privacy. The policy emphasizes the importance of regular data audits to verify compliance and identify areas for improvement, contributing to a privacy-conscious culture that prioritizes both operational efficiency and the protection of sensitive information.

Hardware and Accessories Distribution:

The Hardware and Accessories Distribution policy underscores the IT department's ownership and control over the allocation of hardware resources. All hardware and accessories distribution is exclusively managed by IT, ensuring streamlined ownership, maintenance, and adherence to security standards. Employees seeking hardware must request it through established channels, guaranteeing proper documentation and tracking. This centralized control facilitates efficient resource allocation, reduces redundancy, and ensures compliance with standardized configurations. Regular audits of distributed hardware maintain inventory accuracy. By entrusting the IT department with ownership, this policy promotes responsible and secure hardware distribution, contributing to a well-maintained and optimized technology infrastructure.

Software Licensing and Compliance:

Our Software Licensing and Compliance policy stress the imperative for legal and ethical software use. Users are strictly prohibited from factory resetting any device, ensuring compliance with licensing agreements and preserving authorized software configurations. Software installations must align with approved licenses, preventing unauthorized use and potential legal ramifications. Regular audits monitor compliance, identifying and rectifying any deviations. The IT department oversees licensing documentation and provides guidance to users, fostering a culture of accountability. This ensures that software usage adheres to legal standards, mitigating risks associated with unauthorized modifications, and maintains the integrity of licensed software across all devices.

Disaster Recovery and Incident Response:

Our Disaster Recovery and Incident Response policy encompass comprehensive strategies for safeguarding website, online, and local data. In the event of data loss, the policy outlines a systematic recovery plan, including website restoration protocols and real-time incident response measures. Regular backups of online and local data are conducted, ensuring minimal data loss. The IT department is tasked with overseeing the recovery process, swiftly addressing incidents to minimize downtime and protect critical information. Regular drills and audits are conducted to validate the efficacy of the disaster recovery plan, maintaining readiness to respond effectively to unforeseen events and secure our own and client’s assets.

IT Policy Review and Updates:

Our IT Policy Review and Updates initiative underscore the dynamic nature of our security landscape. Policies are targeted for review every six months, ensuring alignment with evolving industry standards and emerging threats. The IT department, in collaboration with relevant stakeholders,

conducts thorough assessments, identifying areas for enhancement or modification. This proactive approach facilitates the integration of new security measures and technologies. Regular policy reviews not only fortify our defense against potential risks but also foster a culture of continuous improvement, adapting swiftly to changes in the digital landscape and maintaining a resilient IT infrastructure aligned with industry best practices.

Handling and Cleanliness Policy:

Our Handling and Cleanliness Policy prioritizes responsible care of IT equipment while integrating awareness of social engineering risks. Users must exercise caution when handling devices to prevent damage, ensuring optimal working conditions. Regular cleaning of equipment, including keyboards and screens, is encouraged for hygiene. Prohibiting food and beverages near electronic devices prevents spills and potential harm. Additionally, employees are educated on social engineering risks, emphasizing vigilance against manipulative tactics. Any damage or malfunction should be reported promptly to the IT department. Adherence to this policy, along with social engineering awareness, contributes to a secure work environment, fostering efficient and reliable operations.

MAC Address Management Policy:

Our MAC Address Management Policy establishes guidelines for efficiently managing Media Access Control (MAC) addresses within our network. IT is responsible for overseeing and approving the registration and filtering of MAC addresses. All devices connecting to the network must be registered, contributing to enhanced network security. Any changes to MAC addresses require prior approval from IT to prevent unauthorized access and ensure network integrity. Periodic audits and reviews of registered MAC addresses are conducted to identify and address any anomalies, fostering a secure and well-maintained network environment aligned with industry best practices.

MAC Address Filtering and Registration:

Our MAC Address Filtering and Registration policy mandate that employees provide MAC addresses for all devices connecting to the network. IT oversees and approves MAC address registrations, contributing to enhanced network security. Only registered MAC addresses are permitted access, preventing unauthorized connections. Employees must submit MAC addresses for all devices in use, ensuring a comprehensive network inventory. Any changes to MAC addresses require prior IT approval to maintain network integrity. Regular audits and reviews of registered MAC addresses are conducted to identify anomalies, fostering a secure and well-maintained network environment aligned with industry best practices.

Kindly fill out the form below as needed
https://forms.gle/jDQcmUNKSHet4Li57

Device Registration Process:

Our Device Registration Process ensures the systematic onboarding of new assets into our network. Employees are required to complete an asset receiving form for any devices provided to them. This form captures essential details, facilitating accurate record-keeping and inventory management. The IT department oversees this registration process, verifying the information provided and ensuring compliance with security standards. This meticulous approach streamlines device tracking, aids in swift issue resolution, and maintains an accurate inventory. By mandating the asset receiving form, we strengthen our control over device deployment, promoting transparency, and facilitating efficient management of our technological resources.

Updates and Changes:

The Updates and Changes policy governs modifications to our IT infrastructure, ensuring a controlled and secure environment. All updates, whether software or hardware, must be approved by the IT department. This meticulous process guarantees compatibility, mitigates security risks, and maintains system stability. Users are required to report any changes in software configurations promptly. The policy fosters transparency, facilitating efficient communication between users and the IT department. By mandating pre-approval, we prioritize system integrity and protect against potential disruptions, contributing to a well-managed IT ecosystem that aligns with industry best practices and regulatory compliance.

MAC Address Cloning and Impersonation:

Our MAC Address Cloning and Impersonation policy strictly prohibit the unauthorized replication or alteration of MAC addresses. Users are forbidden from engaging in any activity that involves cloning or impersonating MAC addresses, as it poses a significant security risk. The IT department maintains exclusive oversight over MAC address management to prevent misuse and unauthorized access. This policy safeguards the network against potential breaches and ensures the integrity of device identification. Any attempts at MAC address cloning or impersonation are treated as serious violations, subject to disciplinary action. This stringent approach upholds network security, fostering a trusted and secure computing environment.

Regular IT Audits and Reviews with Tagging Protocol:

Our commitment to IT security is upheld through Regular Audits and Reviews, ensuring ongoing evaluation and enhancement of our systems. Quarterly internal IT audits, coupled with yearly external IT audits, meticulously examine security measures, identifying vulnerabilities, and reinforcing compliance. This comprehensive approach includes the tagging of all IT peripherals and tangibles, providing a traceable inventory for effective IT auditing. In-depth IT reviews assess the effectiveness of policies, updating them in response to evolving threats. Continuous monitoring of IT access logs and network activity adds an extra layer of protection. This proactive IT strategy fortifies our defense against potential risks, maintaining a robust approach aligned with industry best practices.

Social Engineering:

Social Engineering is a tactic employed by cyber adversaries to exploit human psychology and manipulate individuals into divulging confidential information or performing actions that compromise security. It often involves deceptive techniques such as phishing emails, impersonation, or pretexting. Users are educated to recognize and resist these tactics, emphasizing the importance of verifying communication authenticity and avoiding divulging sensitive information. Regular training sessions and simulated exercises enhance awareness, ensuring a vigilant workforce capable of identifying and thwarting social engineering attempts. By prioritizing awareness and proactive responses, we strengthen our defense against these sophisticated and prevalent cybersecurity threats.