IT Security and Cloud Data Security Policy

Expert Pensions Consulting Ltd

IT Security and Cloud Data Security Policy

1. Introduction

Expert Pensions Consulting Ltd (the Company) recognises the paramount importance of IT security and cloud data security in protecting sensitive information, ensuring business continuity, and safeguarding customer data. This policy establishes the mandatory principles and explicit guidelines to be adhered to by all employees, contractors, and third parties when accessing, handling, or managing IT systems, infrastructure, and cloud-based services.

2. IT Security Practices

2.1. User Authentication and Access Control

2.1.1. Mandatory Two-Factor Authentication (2FA): All employees must enable and consistently utilise 2FA for all business-related systems and services, including Google Workspace, which serves as the cloud-based application suite for the entire Company.

2.1.2. Robust Password Enforcement: It is mandatory for all users to create and employ strong, complex passwords unique to each account. Password reuse across multiple systems is strictly prohibited. Employees shall employ a secure password management tool to effectively store and manage their passwords.

2.1.3. Rigorous User Account Management: User accounts shall be meticulously created, modified, and disabled based on the principle of least privilege. Access to systems and data will be granted solely on a need-to-know basis.

2.2. Software and System Security

2.2.1. Prompt Patch Management: Regular and expeditious application of security patches and updates to all systems, including operating systems, applications, and network devices, is mandatory to effectively mitigate known vulnerabilities and ensure the integrity of the Company's IT infrastructure.

2.2.2. Uncompromising Malware Prevention: Endpoint protection software must be installed on all devices that access the Company's IT infrastructure. Employees shall promptly report any suspicious software or potential security threats to Rachel Campbell.

2.2.3. Secure Configuration Standardisation: Systems and devices must be meticulously configured in adherence to industry best practices and vendor guidelines to significantly diminish the risk of unauthorised access and data breaches.

2.3. Data Protection and Privacy

2.3.1. Indispensable Encryption Measures: All sensitive data stored in the cloud or transmitted over public networks shall be encrypted using approved encryption algorithms and protocols. The built-in encryption capabilities provided by Google Workspace must be fully utilised whenever applicable.

2.3.2. Prudent Data Classification: Data shall be classified according to its sensitivity and criticality. Access controls, encryption mechanisms, and data handling procedures must be implemented with meticulous adherence to the classification level.

2.3.3. Responsible Data Retention and Disposal: The Company shall establish and rigorously adhere to data retention and disposal procedures that align with legal and regulatory requirements. Data that no longer serves a legitimate business purpose shall be securely and irreversibly eradicated.

3. Cloud Data Security: Assured Google Cloud Security

3.2.1. Inviolable Access Controls: Access to Google Cloud services and data shall be granted solely based on verified business needs and meticulously controlled through the implementation of robust identity and access management (IAM) solutions.
3.2.2. Pragmatic Incident Management: The Company shall maintain a comprehensive incident response plan to promptly address any security incidents related to Google Cloud services. Employees shall immediately report any suspected security incidents to Rachel Campbell for immediate investigation and remediation.
3.2.3. Infallible Backup and Disaster Recovery: Regular backups of critical data stored in Google Cloud shall be diligently performed, and an exhaustive disaster recovery plan must be established to guarantee the availability and integrity of data in the event of any disruptions.

4. Security Awareness and Training
4.1. Mandatory Security Training Program
4.1.1. Thorough Employee Onboarding: All employees, without exception, shall undergo mandatory IT security and privacy training during the onboarding process. This training shall encompass comprehensive instruction on the proper utilisation of Google Workspace and other pertinent systems.
4.1.2. Ongoing Training and Phishing Awareness: Regular security awareness training sessions shall be conducted to reinforce sound security practices, educate employees on emerging threats and vulnerabilities, and specifically address the risks associated with phishing attacks. Employees shall be trained to recognise and immediately report suspicious emails, links, or attachments.
4.2. Strict Compliance Monitoring
4.2.1. Rigorous Policy Enforcement: The Company shall meticulously monitor and enforce compliance with this policy. Non-compliance shall result in appropriate disciplinary action, up to and including termination of employment or contractual agreements.

5. Compliance and Audit
5.1. Full Compliance with Laws and Regulations
5.1.1. Unquestionable Adherence to Security Laws and Regulations: The Company shall demonstrate unequivocal compliance with all applicable security laws and regulations, including data protection and privacy laws, ensuring that all legal requirements are met without compromise.

5.2. Regular Security Audits
5.2.1. Thorough Internal Audits: Rachel Campbell shall conduct regular internal audits to assess compliance with security policies and procedures, diligently identifying any potential areas for improvement and promptly implementing necessary measures.
5.2.2. Independent Audits by Third Parties: Periodic independent security audits may be conducted by external parties to ensure compliance, verify the effectiveness of security controls, and identify any areas requiring further attention.

6. Incident Response and Reporting

6.1. Swift and Methodical Incident Response Plan
6.1.1. Immediate Incident Reporting: All security incidents, breaches, or suspected compromises must be promptly reported to the Rachel Campbell for immediate investigation and remedial action.
6.1.2. Dedicated Incident Response Team: The Company shall establish a specialised incident response team responsible for the prompt and coordinated execution of incident response activities, including containment, eradication, and recovery.
6.2. Transparent Communication and Notification
6.2.1. Comprehensive Communication Plan: The Company shall maintain a well-defined communication plan to ensure timely and accurate dissemination of information related to security incidents, ensuring effective communication with employees, management, customers, and regulatory authorities.
6.2.2. Compliant Data Breach Notification: In the event of a data breach, the Company shall comply fully with all applicable legal and regulatory requirements regarding the notification of affected individuals, customers, and relevant authorities.

7. Policy Review and Updates

7.1. Regular Policy Review
7.1.1. Periodic Policy Review: This policy shall be reviewed and reassessed periodically, at minimum annually, to ensure its ongoing relevance, effectiveness, and alignment with technological advancements, emerging threats, and evolving regulatory requirements.
7.2. Policy Distribution and Employee Acknowledgment
7.2.1. Policy Distribution: This policy shall be disseminated comprehensively to all employees, contractors, and third parties who have access to the Company's IT systems and cloud services, leaving no room for ambiguity or misinterpretation.
7.2.2. Employee Acknowledgment: All users shall be required to explicitly acknowledge and wholeheartedly adhere to this policy as an absolute

Summary of key details about google cloud workspace

- Google prioritises security in its operations and makes it a central aspect of its everyday operations and disaster planning.
- Google has a dedicated security team consisting of experts in various areas of security who maintain defense systems, develop security processes, and conduct security reviews.
- Google collaborates with the security research community and runs Project sero to identify and address vulnerabilities in its products.
- Google employees undergo security and privacy training during the onboarding process and receive ongoing training throughout their careers.
- Google has a dedicated privacy team that ensures privacy requirements are followed in product design and helps release products with strong privacy standards.
- Google has an internal audit team that reviews compliance with security laws and regulations and supports independent audits by third parties.
- Google Cloud provides security controls to protect the privacy and sovereignty of customer data, including access transparency and approval, shielded VMs, and confidential computing.
- Google has vulnerability management programs, malware prevention strategies, security monitoring, and incident management processes in place to ensure operational security.
- Google Cloud runs on a technology platform designed for security, with state-of-the-art data centers and redundant power systems.
- Google data centers have multiple layers of physical security, including access control measures, surveillance cameras, and security patrols.

Please note that the information provided is based on the content you provided, which has a cutoff date of May 2022. There may have been updates or changes to Google's security practices since then.

Google Workspace (formerly G Suite) provides a range of security features to protect user data, but it's important for users to follow best practices and take additional precautions. Here are some tips for enhancing the security of your Google Workspace account:

1. Enable Two-Factor Authentication (2FA): Enable 2FA for your Google Workspace account to add an extra layer of security. This will require a second form of verification, such as a unique code generated by an app or a security key, in addition to your password.

2. Use Strong and Unique Passwords: Create strong, complex passwords for your Google Workspace account and avoid reusing them for other accounts. Consider using a password manager to securely store and manage your passwords.
3. Regularly Update and Patch Software: Keep your operating system, web browsers, and other software up to date with the latest security patches. Regular updates help protect against known vulnerabilities.
4. Be Cautious of Phishing Attempts: Be vigilant of phishing emails or websites that attempt to trick you into revealing your account credentials. Avoid clicking on suspicious links and verify the authenticity of any email requesting sensitive information.
5. Manage Third-Party Access: Review and manage the permissions granted to third-party applications that have access to your Google Workspace data. Remove any unnecessary or unused integrations.
6. Educate and Train Users: Provide security awareness training to educate users about best practices, such as avoiding suspicious emails and practicing good password hygiene. Regularly remind users about the importance of security practices.
7. Monitor Account Activity: Regularly review your account activity and monitor for any suspicious or unauthorised access. Enable alerts for unusual login activity or changes made to your account settings.
8. Encrypt Sensitive Data: Utilise Google Workspace's built-in encryption capabilities to protect sensitive data stored in Google Drive or transmitted through Gmail. This adds an extra layer of protection against unauthorised access.
9. Follow Data Sharing and Access Controls: Implement appropriate data sharing and access controls within your organisation to ensure that sensitive information is only accessible to authorised individuals.
10. Regularly Back Up Data: Create regular backups of important data stored in Google Workspace to protect against data loss or accidental deletion. Consider using Google Vault or third-party backup solutions.

By following these best practices and implementing additional security measures, the highest levels of security are applied to the EPC Google Workspace account.

Expert Pensions Consulting Ltd (the Company) recognises the paramount importance of IT security and cloud data security in protecting sensitive information, ensuring business continuity, and safeguarding customer data for clients.

This policy establishes the explicit guidelines to be adhered to by all employees, contractors, and third parties when accessing, handling, or managing IT systems, infrastructure, and cloud-based services.

Any questions about this policy, please contact us here: hello@expertpensions.com and for the attention of Rachel Campbell, Secretary and Data Protection officer for EPC.