General IT Policies: Artifacts Only Not Presently Adopted

Content Below is from previous policy work and can be imported or adopted for official policies 3.1 - 3.14

Major Document History

Date	Comment	Who
5/6/2019	Initial Doc	Tharp

Control Environment Narrative

The following provides a description of the control structure of DLZP Group. The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor DLZP Group's application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediation's specific to the noted change.

Logical Controls

DLZP Group employs several logical controls to protect confidential data and ensure normal operation of its core product.

- Mandatory data encryption at rest and in motion
- Multi-factor authentication for access to cloud infrastructure
- Activity and anomaly monitoring on production systems
- Vulnerability management program

Policy Controls

DLZP Group employs several policy controls to protect confidential data and ensure normal operation of its core product. These policies include, but are not limited to:

- Access Control Policy
- Encryption Policy
- Office Security Policy
- Password Policy
- Policy Training Policy
- Vendor Policy
- Workstation Policy

Procedural Controls

DLZP Group has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

TODO: Finalize these lists

1. Scheduled Security and Audit Procedures
    1. Review Access [quarterly]
    2. Review Security Logs [weekly]
    3. Review Cyber Risk Assessment (enumerate possible compromise scenarios) [quarterly]
    4. Review Data Classification [quarterly]
    5. Backup Testing [quarterly]
    6. Disaster Recovery Testing [semi-annual]
    7. Review Devices & Workstations [quarterly]
    8. Review & Clear Low-Priority Alerts [weekly]
    9. Apply OS Patches [monthly]
    10. Verify Data Disposal per Retention Policy [quarterly]
    11. Conduct Security Training [annual]
    12. Review Security Monitoring and Alerting Configuration [quarterly]
    13. Penetration Test [annual]
    14. Whitebox Security Review [annual]
    15. SOC2 Audit [annual]
2. Event-Driven Security and Audit Procedures
    1. Onboard Employee
    2. Offboard Employee
    3. Investigate Security Alert
    4. Investigate Security Incident

Remediations

DLZP Group uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. Once identified, these shortcomings are remediated by improving existing controls and procedures, and creating new controls and procedures as needed.

Communications

DLZP Group communicates relevant information regarding the functioning of the above controls with internal and external parties on an as-needed basis and according to statutory requirements.

Internal

DLZP Group communicates control outcomes, anomalies, and remediation's internally using the following channels:

1. Slack
2. Google Hangouts
3. Email
4. ZOHO Ticketing

External

DLZP Group communicates relevant control-related information to external parties including shareholders, customers, contractors, regulators, and government entities as needed according to contractual and regulatory/statutory obligation.

Access Control Policy

People Security - Code of Conduct, Access Control and Confidentiality

Encryption Policy

Purpose and Scope

- This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity and nonrepudiation of information.
- This policy applies to all systems, equipment, facilities and information within the scope of the organization’s information security program.
- All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on behalf of the organization having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must comply with it.

Background

- This policy defines the high level objectives and implementation instructions for the organization’s use of cryptographic algorithms and keys. It is vital that the organization adopt a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

Policy

- The organization must protect individual systems or information by means of cryptographic controls as defined in Table 3:

Table 3: Cryptographic Controls

Name of System/Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Public Key Infrastructure for Authentication	OpenSSL	AES-256	256-bit key
Data Encryption Keys	OpenSSL	AES-256	256-bit key

Name of System/Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Virtual Private Network (VPN) keys	OpenSSL and OpenVPN	AES-256	256-bit key
Website SSL Certificate	OpenSSL, CERT	AES-256	256-bit key

- Except where otherwise stated, keys must be managed by their owners.
- Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorized use and backing up keys on a regular basis.
- When required, customers of the organization’s cloud-based software or platform offering must be able to obtain information regarding:
    1. The cryptographic tools used to protect their information.
    2. Any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions.
    3. The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers’ data.
- The use of organizationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by the Company conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.
- All key management must be performed using software that automatically manages access control, secure storage, backup and rotation of keys. Specifically:
- The key management service must provide key access to specificallydesignated users, with the ability to encrypt/decrypt information and generate data encryption keys.
- The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.
- The key management service must store and backup keys for the entirety of their operational lifetime.
- The key management service must rotate keys at least once every 12 months.

Office Security Policy

Purpose and Scope

1. This policy establishes the rules governing controls, monitoring, and removal of physical access to company’s facilities.
2. This policy applies to all staff, contractors, or third parties who require access to any physical location owned, operated, or otherwise occupied by the company. A separate policy exists for governing access to the company data center.

Policy

1. Management responsibilities
    1. Management shall ensure:
        1. appropriate entry controls are in place for secure areas
        2. security personnel, identification badges, or electronic key cards should be used to validate employee access to facilities

3. confirm visitor & guest access procedure has been followed by host staff
4. management periodically reviews list of individuals with physical access to facilities
5. card access records and visitor logs are kept for a minimum of 90 days and are periodically reviewed for unusual activity

2. Key access & card systems
    1. The following policies are applied to all facility access cards/keys:
        1. Access cards/keys shall not be shared or loaned to others
        2. Access cards/keys shall not have identifying information other than a return mail address
        3. Access cards/keys shall be returned to Human Resources when they are no longer needed
        4. Lost or stolen access cards/keys shall be reported immediately
        5. If an employee changes to a role that no longer requires physical access or leaves the company, their access cards/keys will be suspended
        6. Human Resources will regularly review physical security privileges and review access logs
3. Staff & contractor access procedure
    1. Access to physical locations is granted to employees and contractors based on individual job function and will be granted by Human Resources.
    2. Any individual granted access to physical spaces will be issued a physical key or access key card. Key and card issuance is tracked by Human Resources and will be periodically reviewed.
    3. In the case of termination, Human Resources should ensure immediate revocation of access (i.e. collection of keys, access cards, and any other asset used to enter facilities) through the offboarding procedure.
4. Visitor & guest access procedure
    1. The following policies are applied to identification & authorization of visitors and guests:
        1. All visitors must request and receive written onsite authorization from a staff member.
        2. Visitor access shall be tracked with a sign in/out log. The log shall contain:visitor’s name, firm represented, purpose of visit, and onsite personnel authorizing access
        3. The log shall be retained for a minimum of 90 days
        4. Visitors shall be given a badge or other identification that visibly distinguishes visitors from onsite personnel
        5. Visitor badges shall be surrendered before leaving the facility
5. Audit controls & management
    1. Documented procedures and evidence of practice should be in place for this policy. Acceptable controls and procedures include:
        1. visitor logs
        2. access control procedures
        3. operational key-card access systems
        4. video surveillance systems (with retrievable data)
        5. ledgers if issuing physical keys
6. Enforcement
    1. Employees, contractors, or third parties found in violation of this policy (whether intentional or accidental) may be subject to disciplinary action, including:
        1. reprimand
        2. loss of access to premises
        3. termination

Password Policy

Purpose and Scope

1. The Password Policy describes the procedure to select and securely manage passwords.
2. This policy applies to all employees, contractors, and any other personnel who have an account on any system that resides at any company facility or has access to the company network.

Policy

1. Rotation requirements
    1. All system-level passwords should be rotated on at least a quarterly basis. All user-level passwords should be rotated at least every six months.
    2. If a credential is suspected of being compromised, the password in question should be rotated immediately and the Engineering/Security team should be notified.
2. Password protection
    1. All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, deny the request and contact the system owner for assistance in provisioning an individual user account.
    2. Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone. If you must store passwords electronically, do so with a password manager that has been approved by IT. If you truly must share a password, do so through a designated password manager or grant access to an application through a single sign on provider.
    3. Do not use the “Remember Password” feature of applications and web browsers.
    4. If you suspect a password has been compromised, rotate the password immediately and notify engineering/security.
3. Enforcement
    1. An employee or contractor found to have violated this policy may be subject to disciplinary action.

Policy Training Policy

Purpose and Scope

1. This policy addresses policy education requirements for employees and contractors.
2. This policy applies to all full-time employees, part-time employees, and contractors. Adherence to assigned policies is binding under their Employment Offer Letter and/or Independent Contractor Agreement.

Applicability

1. Upon hire of a new employee or contractor, the Hiring Manager will determine which subsets of policies will apply to that individual. The individual will have five working days to read the assigned policies. The following will be logged in the Policy Training Policy Ledger:
    1. Assignment date

2. Completion date
3. Policy
4. Assignee
5. Assigner
6. Notes

Vendor Policy

Purpose and Scope

1. This policy defines the rules for relationships with the organization’s Information Technology (IT) vendors and partners.
2. This policy applies to all IT vendors and partners who have the ability to impact the confidentiality, integrity, and availability of the organization’s technology and sensitive information, or who are within the scope of the organization’s information security program.
3. This policy applies to all employees and contractors that are responsible for the management and oversight of IT vendors and partners of the organization.

Background

1. The overall security of the organization is highly dependent on the security of its contractual relationships with its IT suppliers and partners. This policy defines requirements for effective management and oversight of such suppliers and partners from an information security perspective. The policy prescribes minimum standards a vendor must meet from an information security standpoint, including security clauses, risk assessments, service level agreements, and incident management.

References

1. Information Security Policy
2. Security Incident Response Policy

Policy

1. IT vendors are prohibited from accessing the organization’s information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.
2. All IT vendors must comply with the security policies defined and derived from the Information Security Policy (reference (a)).
3. All security incidents by IT vendors or partners must be documented in accordance with the organization’s Security Incident Response Policy (reference (b)) and immediately forwarded to the Information Security Manager (ISM).
4. The organization must adhere to the terms of all Service Level Agreements (SLAs) entered into with IT vendors. As terms are updated, and as new ones are entered into, the organization must implement any changes or controls needed to ensure it remains in compliance.
5. Before entering into a contract and gaining access to the parent organization’s information systems, IT vendors must undergo a risk assessment.
    1. Security risks related to IT vendors and partners must be identified during the risk

assessment process.
    2. The risk assessment must identify risks related to information and communication technology, as well as risks related to IT vendor supply chains, to include sub-suppliers.
6. IT vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. The organization strictly adheres to all applicable legal, regulatory and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally-Identifiable Information (PII).
7. The organization may choose to audit IT vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory and contractual obligations.

Workstation Policy

Purpose and Scope

1. This policy defines best practices to reduce the risk of data loss/exposure through workstations.
2. This policy applies to all employees and contractors. Workstation is defined as the collection of all company-owned and personal devices containing company data.

Policy

1. Workstation devices must meet the following criteria:
    1. Operating system must be no more than one generation older than current
    2. Device must be encrypted at rest
    3. Device must be locked when not in use or when employee leaves the workstation
    4. Workstations must be used for authorized business purposes only
    5. Loss or destruction of devices should be reported immediately
    6. Laptops and desktop devices should run the latest version of antivirus software that has been approved by IT
2. Desktop & laptop devices
    1. Employees will be issued a desktop, laptop, or both by the company, based on their job duties. Contractors will provide their own laptops.
    2. Desktops and laptops must operate on macOS or Windows.
3. Mobile devices
    1. Mobile devices must be operated as defined in the Removable Media Policy, Cloud Storage, and Bring Your Own Device Policy.
    2. Mobile devices must operate on iOS or Android.
    3. Company data may only be accessed on mobile devices with Slack and Gmail.
4. Removable media
    1. Removable media must be operated as defined in the Removable Media Policy, Cloud Storage, and Bring Your Own Device Policy.
    2. Removable media is permitted on approved devices as long as it does not conflict with other policies.

Logging and Monitoring Policy

Purpose and Scope

1. This policy defines best practices .....
2. This policy applies to all employees and contractors. ....

Policy

1. Logging devices must meet the following criteria:
    1. Operating system must be no more than one generation older than current
    2. Device must be encrypted at rest
    3. Device must....

Tranche 2

Control Environment Narrative

The following provides a description of the control structure of DLZP Group. The intent of this description is to enumerate the logical, policy, and procedural controls that serve to monitor DLZP Group's application and data security. Changes uncovered by these procedures in the logical, policy, procedural, or customer environment are addressed by remediation's specific to the noted change.

Purpose and Scope

- Use non-privileged accounts or roles when accessing non-security functions.
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
- Limit unsuccessful logon attempts.
- Provide privacy and security notices consistent with applicable rules.
- Use session lock with pattern- hiding displays to prevent access and viewing of data after a period of inactivity.
- Terminate (automatically) a user session after a defined condition.
- Monitor and control remote access sessions.
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
- Route remote access via managed access control points.

Logical Controls

DLZP Group employs several logical controls to protect confidential data and ensure normal operation of its core product.

- Mandatory data encryption at rest and in motion
- Multi-factor authentication for access to cloud infrastructure
- Activity and anomaly monitoring on production systems
- Vulnerability management program

Policy Controls

DLZP Group employs several policy controls to protect confidential data and ensure normal operation of its core product. These policies include, but are not limited to:

- Access Control Policy
- Encryption Policy
- Office Security Policy
- Password Policy
- Policy Training Policy
- Vendor Policy
- Workstation Policy

Procedural Controls

DLZP Group has numerous scheduled procedures to monitor and tune the effectiveness of ongoing security controls, and a series of event-driven procedures to respond to security-related events.

TODO: Finalize these lists

1. Onboarding Checklist
    1. Email Access
    2. File Storage Access
    3. PC Access
        1. VPN
    4. App Access
        1. Google Apps
        2. Microsoft Office365
        3. ZOHO Apps
        4. Slack
        5. WIKI
2. Offboarding Checklist
    1. Email Termination
    2. File Storage Termination
    3. PC Access
        1. VPN
    4. Corp Apps Access
        1. Google Apps
        2. Microsoft Office365
        3. ZOHO Apps
        4. Slack
        5. WIKI
3. Scheduled Security and Audit Procedures
    1. Review Access [quarterly]
    2. Review Security Logs [weekly]
    3. Review Cyber Risk Assessment (enumerate possible compromise scenarios) [quarterly]
    4. Review Data Classification [quarterly]
    5. Backup Testing [quarterly]
    6. Disaster Recovery Testing [semi-annual]
    7. Review Devices & Workstations [quarterly]

8. Review & Clear Low-Priority Alerts [weekly]
9. Apply OS Patches [monthly]
10. Verify Data Disposal per Retention Policy [quarterly]
11. Conduct Security Training [annual]
12. Review Security Monitoring and Alerting Configuration [quarterly]
13. Penetration Test [annual]
14. Whitebox Security Review [annual]
15. SOC2 Audit [annual]

4. Event-Driven Security and Audit Procedures
    1. Onboard Employee
    2. Offboard Employee
    3. Investigate Security Alert
    4. Investigate Security Incident

Remediations

DLZP Group uses the outcomes of the aforementioned controls and procedures to identify shortcomings in the existing control environment. Once identified, these shortcomings are remediated by improving existing controls and procedures, and creating new controls and procedures as needed.

Communications

DLZP Group communicates relevant information regarding the functioning of the above controls with internal and external parties on an as-needed basis and according to statutory requirements.

Internal

DLZP Group communicates control outcomes, anomalies, and remediation's internally using the following channels:

1. Slack
2. Email
3. ZOHO Ticketing

External

DLZP Group communicates relevant control-related information to external parties including shareholders, customers, contractors, regulators, and government entities as needed according to contractual and regulatory/statutory obligation.

Access, Onboarding and Termination Policy

Purpose and Scope

- The purpose of this policy is to define procedures to onboard and offboard users to technical infrastructure in a manner that minimizes the risk of information loss or exposure.
- This policy applies to all technical infrastructure within the organization.
- This policy applies to all full-time and part-time employees and contractors.
- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
- Limit system access to the types of transactions and functions that authorized users are permitted to execute.
- Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
- Employ the principle of least privilege, including for specific security functions and privileged accounts.

Background

- In order to minimize the risk of information loss or exposure (from both inside and outside the organization), the organization is reliant on the principle of least privilege. Account creation and permission levels are restricted to only the resources absolutely needed to perform each person’s job duties. When a user’s role within the organization changes, those accounts and permission levels are changed/revoked to fit the new role and disabled when the user leaves the organization altogether.
- All users within DLZP Group are provided with a unique Authentication Account. This account is the primary means of the user accessing DLZP resources. The same account ID is used across all systems.

Policy

During onboarding:

- Hiring Manager informs HR upon hire of a new employee.
- HR emails IT to inform them of a new hire and their role.
- IT creates a checklist of accounts and permission levels needed for that role.
- The User is assigned a unique id consisting of their [firstname.lastname].
- The owner of each resource reviews and approves account creation and the associated permissions.
- IT works with the owner of each resource to set up the user.

During offboarding:

- Hiring Manager notifies HR when an employee has been terminated.
- HR sends a weekly email report to IT summarizing list of users terminated and instructs IT to disable their access.
- IT terminates access within five business days from receipt of notification.

When an employee changes roles within the organization:

- Hiring Manager will inform HR of a change in role.
- HR and IT will follow the same steps as outlined in the onboarding and offboarding procedures.

- Review of accounts and permissions:
- Each month, IT and HR will review accounts and permission levels for accuracy.

Password Policy

Purpose and Scope

1. The Password Policy describes the procedure to select and securely manage passwords.
2. This policy applies to all employees, contractors, and any other personnel who have an account on any system that resides at any company facility or has access to the company network.

Policy

1. Rotation requirements
    1. All system-level passwords should be rotated on at least a quarterly basis. All user-level passwords should be rotated at least every six months.
    2. If a credential is suspected of being compromised, the password in question should be rotated immediately and the Engineering/Security team should be notified.
2. Password protection
    1. All passwords are treated as confidential information and should not be shared with anyone. If you receive a request to share a password, deny the request and contact the system owner for assistance in provisioning an individual user account.
    2. Do not write down passwords, store them in emails, electronic notes, or mobile devices, or share them over the phone. If you must store passwords electronically, do so with a password manager that has been approved by IT. If you truly must share a password, do so through a designated password manager or grant access to an application through a single sign on provider.
    3. Do not use the “Remember Password” feature of applications and web browsers.
    4. If you suspect a password has been compromised, rotate the password immediately and notify engineering/security.
3. Enforcement
    1. An employee or contractor found to have violated this policy may be subject to disciplinary action.

Encryption Policy

Purpose and Scope

- This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity and nonrepudiation of information.
- This policy applies to all systems, equipment, facilities and information within the scope of the organization’s information security program.
- All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on behalf of the organization having to do with cryptographic systems, algorithms, or keying material are subject to this policy and must

comply with it.

Background

- This policy defines the high level objectives and implementation instructions for the organization's use of cryptographic algorithms and keys. It is vital that the organization adopt a standard approach to cryptographic controls across all work centers in order to ensure end-to-end security, while also promoting interoperability. This document defines the specific algorithms approved for use, requirements for key management and protection, and requirements for using cryptography in cloud environments.

Policy

- The organization must protect individual systems or information by means of cryptographic controls as defined in Table 3:

Table 3: Cryptographic Controls

Name of System/Type of Information	Cryptographic Tool	Encryption Algorithm	Key Size
Public Key Infrastructure for Authentication	OpenSSL	AES-256	256-bit key
Data Encryption Keys	OpenSSL	AES-256	256-bit key
Virtual Private Network (VPN) keys	OpenSSL and OpenVPN	AES-256	256-bit key
Website SSL Certificate	OpenSSL, CERT	AES-256	256-bit key

- Except where otherwise stated, keys must be managed by their owners.
- Cryptographic keys must be protected against loss, change or destruction by applying appropriate access control mechanisms to prevent unauthorized use and backing up keys on a regular basis.
- When required, customers of the organization's cloud-based software or platform offering must be able to obtain information regarding:
    1. The cryptographic tools used to protect their information.
    2. Any capabilities that are available to allow cloud service customers to apply their own cryptographic solutions.
    3. The identity of the countries where the cryptographic tools are used to store or transfer cloud service customers' data.
- The use of organizationally-approved encryption must be governed in accordance with the laws of the country, region, or other regulating entity in which users perform their work. Encryption must not be used to violate any laws or regulations including import/export restrictions. The encryption used by the Company conforms to international standards and U.S. import/export requirements, and thus can be used across international boundaries for business purposes.
- All key management must be performed using software that automatically manages access control, secure storage, backup and rotation of keys. Specifically:
- The key management service must provide key access to specificallydesignated users, with the ability to encrypt/decrypt information and generate data encryption keys.
- The key management service must provide key administration access to specifically-designated users, with the ability to create, schedule delete, enable/disable rotation, and set usage policies for keys.

- The key management service must store and backup keys for the entirety of their operational lifetime.
- The key management service must rotate keys at least once every 12 months.

Remote Access Policy

Purpose and Scope

The purpose of this policy is to provide guidance on the use of Remote Access VPN.

Background

- DLZP Group is 100% Telework and therefore requires all user to access systems from remote locations.
- DLZP Utilizes VPN Software to provide access to systems that are hosted and managed by DLZP Group.
- Resources that are provided using SAAS Software are protected using secure authentication into those services.

Policy

From:
https://wiki.cloud.dlzpgroup.com/ -

Permanent link:
https://wiki.cloud.dlzpgroup.com/doku.php?id=corpgov:physical

Last update: **2019/09/19 17:43**