3.9 HR Policies; People Security - Code of Conduct and Confidentiality

NIST PS Control Standards Spread Sheet

Links

Executive Governance

Control Satisfaction Matrix

Standard	NIST Category	Controls Satisfied	A-lign Controls
DLZP Internal	Family	N/A	2.0, 6.0, 11.0, 16.0

Major Document History

Date	Comment	Who
5/1/2019	Initial Doc	Tharp
7/24/2019	Added Wireless Communications Policies - 27.0	Tharp
7/26/2019	Added Acceptable Use Policy - 2.0 , Email Policy - 6.0	Tharp
7/30/2019	Added 11.0, 16.0	Tharp
8/09/2019	Updated 6.5, 11.5, 16.5	Tharp
8/12/2019	Removed 27.0, Format.	Tharp
8/14/2019	Removed bullet points	Evanko
8/29/19	Edited Code of Conduct - bullet points g and l	Evanko
9/4/19	Edited 11.3.2, 11.3.3, 11.5, 16.1, 16.3, 16.3.1, 16.3.2,	Evanko
9/4/19	Edited Confidentiality Policy 2, 3	Evanko
10/6/2021	Policy's Reviewed for Audit	Tharp

Code of Conduct Policy

Purpose and Scope

1. The purpose of this policy is to define expected behavior from employees towards their colleagues, supervisors, and the overall organization.
2. We expect all employees to follow our Code of Conduct. Offensive behavior, disruptive behavior, and participation in serious disputes should be avoided. Employees are expected to foster a respectful and collaborative environment.
3. This policy applies to all employees and contractors. They are bound by their Employment Offer Letter or Independent Contractor Agreement to follow the Code of Conduct Policy while performing their duties. The Code of Conduct is outlined below:

1. Respect in the workplace
    1. Employees should respect their colleagues. Discriminatory behavior, harassment, or victimization will not be tolerated.
2. Personal appearance
    1. When in the workplace, employees must present themselves in an appropriate & professional manner. They should abide by the company dress code.
3. Corruption
    1. Employees are discouraged from accepting gifts from clients or partners. Briberies are prohibited for the benefit of any external or internal party.
4. Job duties and authority
    1. Employees should fulfill their job duties with integrity and respect towards all individuals involved.
    2. Supervisors and managers may not use abuse their authority. Competency and workload should be taken into account when delegating duties to team members.
    3. Team members are expected to follow their leaders' instructions and complete their duties with thoughtfulness and in a timely manner.
5. Absenteeism and tardiness
    1. Employees should be punctual when coming to and leaving from work and follow the schedule determined by their hiring manager. Exceptions can be made for occasions that prevent employees from following standard working hours or days, with approval from their hiring manager.
    2. Employees are expected to be punctual when attending events representing the company.
6. Conflict of interest
    1. Employees should avoid any personal, financial, or other interests that might compete with their job duties.
7. Collaboration
    1. Employees should be friendly with their colleagues and open to collaboration. They should not disrupt the workplace or present obstacles to their colleagues' work.
8. Communication
    1. Colleagues, supervisors, or team members must be open to communication amongst each other.
9. Benefits
    1. We expect employees to not abuse their employment benefits. This can refer to time off, insurance, facilities, subscriptions, or other benefits our company offers. Refer to Human Resources for more information on benefits.
10. Policies
    1. All employees must comply with company policies. Questions should be directed to their hiring managers and/or Human Resources.
11. Disciplinary actions
    1. Repeated or intentional violation of the Code of Conduct Policy will be met with disciplinary action. Consequences will vary depending on the violation, but can include:
        1. demotion
        2. reprimand
        3. suspension or termination
        4. detraction of benefits for a definite or indefinite time
    2. Cases of corruption, theft, embezzlement, or other unlawful behavior may call for legal action.
12. Social Media
    1. Employees may not post financial, confidential, sensitive or proprietary information

about the Company, clients, employees or applicants.
2. Employees may not post obscenities, slurs or personal attacks that can damage the reputation of the Company, clients, employees or applicants.
3. When posting on social media sites, employees must use the following disclaimer when discussing job-related matters, “The opinions expressed on this site are my own and do not necessarily represent the views of DLZP Group.”
4. DLZP Group may monitor content out on the Internet. Policy violations may result in discipline up to and including termination of employment.

Confidentiality

Purpose and Scope

- This policy outlines expected behavior of employees to keep confidential information about clients, partners, and our company secure.
- This policy applies to all employees, board members, investors, and contractors, who may have access to confidential information. This policy must be made readily available to all whom it applies to.

Background

1. The company’s confidential information must be protected for two reasons:
    1. It may be legally binding (i.e. sensitive customer data)
    2. It may be fundamental to our business (i.e. business processes)
2. Common examples of confidential information in our company includes, but is not limited to:
    1. Unpublished financial information
    2. Customer/partner/vendor/external party data
    3. Patents, formulas, new technologies, and other intellectual property
    4. Existing and prospective customer lists
    5. Undisclosed business strategies including pricing & marketing
    6. Materials & processes explicitly marked as “confidential”
3. Employees will have varying levels of authorized access to confidential information.

Policy

1. Employee procedure for handling confidential information
    1. Lock and secure confidential information at all times
    2. Safely dispose (i.e. shred) documents when no longer needed
    3. View confidential information only on secure devices
    4. Disclose information only when authorized and necessary
    5. Do not use confidential information for personal gain, benefit, or profit
    6. Do not disclose confidential information to anyone outside the company or to anyone within the company who does not have appropriate privileges
    7. Do not store confidential information or replicates of confidential information in unsecured manners (i.e. on unsecured devices)
    8. Do not remove confidential documents from company’s premises unless absolutely

necessary to move
2. Separation of Employment measures
    1. The Hiring Manager should confirm the Separation of Employment procedure has been completed by final date of employment.
3. Confidentiality measures
    1. The company will take the following measures to ensure protection of confidential information:
        1. Encrypt electronic information and implement appropriate technical measures to safeguard databases
        2. Require employees to sign non-disclosure/non-compete agreements
        3. Consult with senior management before granting employees access to certain confidential information
4. Exceptions
    1. Under certain legitimate conditions, confidential information may need to be disclosed. Examples include:
        1. If a regulatory agency requests information as part of an audit or investigation
        2. If the company requires disclosing information (within legal bounds) as part of a venture or partnership
    2. In such cases, employee must request and receive prior written authorization from their hiring manager before disclosing confidential information to any third parties.
5. Disciplinary consequences
    1. Employees who violate the confidentiality policy will face disciplinary and possible legal action.
    2. A suspected breach of this policy will trigger an investigation. Intentional violations will be met with termination and repeated unintentional violations may also face termination.
    3. This policy is binding even after the termination of employment.

2.0 Acceptable Use Policy

2.1 Overview

DLZP Group’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to DLZP Group’s established culture of openness, trust and integrity. DLZP Group is committed to protecting our employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of DLZP Group. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every DLZP Group employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. Security procedures are sought from many external sources on an ongoing basis to stay current with new technologies and systems.

2.2 Purpose

This policy outlines the acceptable use of computer equipment at DLZP Group for the purpose of protecting DLZP Group, DLZP Group's employees, clients, and partners. Inappropriate use exposes DLZP Group to risks including virus attacks, compromise of network systems and services, and legal issues.

2.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at DLZP Group, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DLZP Group.

2.4 Policy

2.4.1 General Use and Ownership

1. All data that users create on the corporate systems remains the property of DLZP Group. Management does not guarantee the confidentiality of personal information stored on any network device belonging to DLZP Group.
2. Employees should exercise good judgment regarding the personal use of company assets. In the absence of such policies, employees should be guided by departmental policies on personal use. For questions regarding acceptable usage, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within DLZP Group may monitor equipment, systems and network traffic at any time.
4. DLZP Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4.2 Security and Proprietary Information

1. The information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the Information Sensitivity policy. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords must be changed at least every 42 days for domain accounts and 90 days for Connections accounts.
3. All users are required to lock the screen (control-alt-delete for Win2K/XP users) of their PC, laptop, or workstation when it will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a DLZP Group email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DLZP Group, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the DLZP Group Internet/Intranet/Extranet, whether owned by the employee or DLZP Group, shall be continually

executing approved virus-scanning software (Symantec Corporate Antivirus Protection) with current virus definitions.
7. Employees should avoid or must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Trojans, or other forms of malware.

2.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of DLZP Group authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DLZP Group-owned resources. The list items below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by DLZP Group.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DLZP Group or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, etc.).
5. Revealing account passwords to others or allowing others usage of an account not their own. This includes family and other household members when work is being done at home.
6. Using a DLZP Group computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any DLZP Group account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to DLZP Group is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, DLZP Group employees to parties outside DLZP Group unless it is a part of normal job duties.

2.5 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within DLZP Group’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DLZP Group or connected via DLZP Group’s network.
7. Posting the same or similar non-business-related messages to large numbers of email recipients (spam).

2.6 Enforcement

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

2.7 Spam

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

6.0 Automatically Forwarded Email Policy

6.1 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

6.2 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of DLZP Group.

6.3 Policy

Employees must exercise utmost caution when sending any email from inside DLZP Group to an outside network. Unless approved by an employee's manager, DLZP Group’s email will not be automatically forwarded to an external destination. Sensitive information, as defined in the Information Sensitivity Policy, will not be forwarded via any means, unless that email is critical to business.

6.4 Enforcement

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

6.5 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to DLZP Group or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

11.0 Email Retention Policy

11.1 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction. Questions about the retention of a specific piece of information should be addressed to a manager. Questions about these guidelines should be addressed to the Internal Help Desk.

11.2 Scope

IT provides the infrastructure for departments to retain emails. Each department is responsible for retaining its own emails according to its own policies.

11.3 Policy

11.3.1 Categories of Correspondence

- Categories of correspondence that users should use when considering whether to retain an email include:
- Administrative – clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations.
- Fiscal – information related to revenue and expense for the company.
- Ephemeral – personal email, requests for recommendations or review, email related to product development, updates and status reports.
- General – information that relates to customer interaction and the operational decisions of the business.
- Protected Health Information – any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

11.3.2 Instant Messenger Correspondence

DLZP Group Instant Messenger includes Google Hangout and Slack. Important conversations should be copied and saved in a file on a backed up drive or in an email.

11.3.3 Server Email Retention and Backup

DLZP Group does not purge the email server of old emails. AWS Workmail is our provider of record for email storage and backup. All email is journaled and replicated to another account. All email events are logged and stored in aws cloudwatch/s3.

11.4 Enforcement

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

11.5 Definitions

Term	Definition
Approved Electronic Mail	Includes all mail systems supported by Systems & Security. For business needs that require the use of other systems, contact the appropriate support organization.
Approved Instant Messenger	Google Hangouts, Slack and Text are the only IM clients approved for internal DLZP Group communications.

Term	Definition
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac's and PCs, this includes using passwords on screensavers.
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of DLZP Group.

16.0 Information Sensitivity Policy

16.1 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of DLZP Group without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that employees can take to protect DLZP Group Confidential information (e.g., DLZP Group Confidential information should not be left unattended anywhere.

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to a manager. Questions about these guidelines should be addressed to Human Resources.

16.2 Scope

All DLZP Group information is categorized into two main classifications:

- DLZP Group Public
- DLZP Group Confidential
- Client Confidential (subset of DLZP Group Confidential)

DLZP Group Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to DLZP Group, Inc.

DLZP Group Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in DLZP Group Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not

require as stringent a degree of protection.

A subset of DLZP Group Confidential information is “Client Confidential” information. This is confidential information belonging or pertaining to another corporation which has been entrusted to DLZP Group by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into DLZP Group’s network to support our operations.

DLZP Group personnel are required to secure DLZP Group Confidential (as well as subset Client Confidential) information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager immediately.

16.3 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as DLZP Group Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the DLZP Group Confidential information in question.

Marking is at the discretion of the owner or custodian of the information. Even if no marking is present, DLZP Group information is presumed to be “DLZP Group Confidential” unless expressly determined to be DLZP Group Public information by DLZP Group Executive Management.

16.3.1 Minimal Sensitivity – “DLZP Group Public”: General corporate information; some personnel and technical information

- Access: DLZP Group employees, contractors, people with a business need to know.
- Distribution within DLZP Group: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
- Distribution outside of DLZP Group internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
- Electronic distribution: No restrictions except that it be sent to only approved recipients.
- Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
- Disposal/Destruction: electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

16.3.2 More Sensitive – “DLZP Group Confidential”: Business, financial, technical, and most personnel information

- Access: DLZP Group employees and non-employees with signed non-disclosure agreements who have a business need to know.
- Distribution within DLZP Group: approved electronic mail and electronic file transmission

methods.
- Distribution outside of DLZP Group internal mail: Sent via U.S. mail or approved private carriers.

16.3.3 Electronic distribution: No restrictions to approved recipients within DLZP Group, but should be encrypted or sent via a private link to approved recipients outside of DLZP Group premises.

- Storage: Individual access controls are highly recommended for electronic information.
- Disposal/Destruction: In disposal bins on DLZP Group premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

16.3.4 Most Sensitive – Elements of “DLZP Group Confidential” and all “Client Confidential”: Trade secrets & marketing, operational, personnel, financial, source code, & technical Information integral to the success of our company and all Client Confidential Data

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of “3rd Party Confidential”. To indicate that DLZP Group Confidential information is very sensitive, consider labeling the information with “DLZP Group Internal: Registered and Restricted”, “DLZP Group Eyes Only”, “DLZP Group Confidential” or similar labels as deemed by the affected individual business unit or department. Once again, this type of DLZP Group Confidential information need not be marked, but users should be aware that this information is extremely sensitive and must be protected as such.

- Access: Only those individuals (DLZP Group employees and non-employees) designated with approved access and signed non-disclosure agreements.
- Distribution within DLZP Group: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
- Distribution outside of DLZP Group internal mail: Delivered direct; signature required; approved private carriers.
- Electronic distribution: No restrictions to approved recipients within DLZP Group, but all “Confidential” information must be strongly encrypted.
- Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
- Disposal/Destruction: Strongly Encouraged: In disposal bins on DLZP Group premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
- Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

16.4 Enforcement

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

16.5 Definitions

Terms	Definitions
Appropriate measures	To minimize risk to DLZP Group from an outside business connection, DLZP Group computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access DLZP Group corporate information, the amount of information at risk is minimized.
Configuration of DLZP Group-to-other business connections	Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.
Approved Electronic File Transmission Methods	Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential	Special envelopes are not required. Put the document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes all mail systems supported by the Network Administrator. These include, but are not necessarily limited to Microsoft Exchange and Outlook. For business needs that require the use of other mailers contact the appropriate support organization.
Approved Encrypted email and files	Techniques include the use of PGP or GPG. DES encryption is available via many different public domain packages on all platforms. Please contact the Help Desk regarding approved encryption methods.
Company Information System Resources	Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
Expunge	To reliably erase or expunge data on a PC, a separate program must overwrite data. Otherwise, the PC’s normal erasure routine keeps the data intact until overwritten.
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On PCs, this includes using passwords on screensavers.
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of DLZP Group.
Encryption	Secure DLZP Group Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult the Help Desk for further guidance.
Physical Security	Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state. Methods of accomplishing this include having a domain username and password to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or keep it in person. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet. No information, equipment, or software belonging to DLZP Group shall be removed from the premises without express authorization from executive management.
Private Link	A Private Link is an electronic communications path that DLZP Group has control over its entire distance. For example, all DLZP Group networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. Connections to employee’s homes are private links.