-English Translation -

Information Technology Security Policy and Guidelines

Pinthong Industrial Park Public Company Limited

Revision No.6

13 November 2024

Approved on 13 November 2024, BOD4/2024

Contents

	Page
Information Technology Security Policy and Guidelines	
1. Objectives	**1**
2. Scope	**1**
3. Computer Control	**2**
3.1) Introduction of Computer Equipment and Storage Media for Use	2
3.2) Repair of Computer Equipment and Storage Media	3
3.3) Disposal of Computer Equipment and Storage Media	3
4. Computer Usage Practices	**4**
4.1) General Practices	4
4.2) Security Measures	5
4.3) Password Control Measures for Usage	6
4.4) Use of Notebook Computers Outside the Company	6
5. Network System	**7**
5.1) General Information	7
5.2) E-mail System	8
5.3) Website System	9
6. Policy on Personal Data Management Stored in Computer Systems	**10**
6.1) Types of Data Collected	10
6.2) Purpose of Personal Data Processing	10
6.3) Disclosure of Personal Data	12
6.4) Consent and Data Subject Rights	13
6.5) Data Retention Period	13
6.6) Compliance with Personal Data Management Policy	14
7. Control of Service Providers for System Management	**14**
8. Precautions Regarding Information Systems	**15**
9. User Account Control	**15**
10. Handling of Unexpected Incidents	**16**
11. Others	**16**
12. Appendix A: A: ERP System Username Details	**18**
Linux ERPPROD และ ERPPRODDB	

Information Technology Security Policy and Guidelines

1. Objectives

The Information Technology Security Policy and Guidelines establish rules and regulations to prevent incidents in the use of information assets of Pinthong Industrial Park Public Company Limited and its subsidiaries (the "Company"), such as unauthorized modification of data, data damage, and data leakage, whether intentional or unintentional. All users of the Company's information assets shall recognize the importance of information security and shall strictly comply with this policy.

2. Scope

2.1) Definition of Information Assets

Information Assets shall mean information systems or data used within information systems.

Information System shall mean a system in which computers are utilized to collect, store, or manage data in order to transform such data into meaningful information that can be processed and used to support decision-making in operations efficiently and in a timely manner. An information system shall therefore consist of key components, namely hardware, software, users, data, and procedures.

Computer shall mean computer equipment, servers, personal computers, portable data devices (such as tablets or mobile phones), peripheral devices, and storage devices (such as magnetic disks), comprising both hardware and software.

Hardware shall mean the physical components of a computer system, which are generally divided into three main parts:

(1) Input devices, such as keyboards and data input units

(2) Memory units, which are used for data storage

(3) Output devices, such as monitors and printers, this shall also include other related physical equipment.

Software shall mean computer programs or sets of instructions written in any computer programming language that can be interpreted and executed by a computer to perform specified tasks within the capabilities of such computer or program.

Data shall mean electronic data within network systems or information systems.

Network shall mean a system in which at least two computers are interconnected through communication media, enabling efficient data exchange among users. Such systems include Local Area Networks (LAN), Wireless Networks (Wi-Fi or Wireless Fidelity), or Wireless LAN (WLAN)

2.2) Persons Subject to the Policy

This Information Technology Security Policy and Guidelines shall apply to all directors, executives, and employees of the Company, including any persons authorized to access and use the Company's information assets under appropriate supervision and control, as deemed appropriate by the designated responsible person.

2.3) Equipment Subject to the Policy

This Information Technology Security Policy and Guidelines shall cover all information systems equipment and information assets owned by the Company, including computers, network devices, equipment from external entities, employees' personal computers, and contractors' computers used in the Company's operations, which are authorized for use under appropriate supervision and control, as deemed appropriate by the designated responsible person.

3. Computer Control

3.1) Introduction of Computer Equipment and Storage Media for Use

1) The use of computers or software-related equipment without prior authorization from the ICT Department is strictly prohibited.
2) The type of equipment selected must always include appropriate security protection systems, such as antivirus software approved and used by the Company.
3) In the case of installing servers and computers, suppliers/contractors must be selected who are capable of providing onsite services, in order to prevent data leakage and to ensure the protection of the Company's confidential information in accordance with this Policy.

4) For software to be installed on servers and computers, the ICT Department shall control the number of licenses and the number of installed machines in actual use, and shall properly retain warranty documents and storage media.
5) Company computers shall not be permitted to use external storage devices, such as flash drives or external hard disks.
6) Other Company recording devices that are regularly used, such as drones or cameras, must be reported to the ICT Department for registration (device serial locking) in order to enable data transfer into Company computers.
7) In cases where the use of external storage devices under Clause 5) is required, a request must be submitted through the ICT work system to obtain temporary authorization for unlocking such usage.

3.2) Repair of Computer Equipment and Storage Media

1) In the event of computer malfunction, the ICT Department shall be responsible for overseeing repairs, subject to ICT approval.
2) It is prohibited to send computer equipment for repair outside the Company. The ICT Department shall coordinate with suppliers/contractors to perform onsite repairs. In cases where it is necessary to send equipment outside the Company, storage devices such as hard disks must not be taken out; they shall be removed and retained within the Company.
3) In cases where it is necessary to repair storage devices (e.g., hard disks) outside the Company, only reliable suppliers/contractors shall be selected.

3.3 Disposal of Computer Equipment and Storage Media

1) Disposal of computer equipment must be approved by the ICT Department in advance, and the ICT Department shall comply with the procedures for disposal of deteriorated assets in accordance with the asset registration and inspection procedures of the Asset Registration Department.
2) The ICT Department shall be responsible for the destruction of storage media, such as hard disks, by ensuring that all data contained therein is completely erased or that the

storage media is physically destroyed prior to disposal. Procedures for data erasure shall vary depending on each type of storage media.

Type of Storage Media	Data Erasure Procedure	Media Destruction Procedure
1) **Optical Media** (e.g., CD, DVD, BD)	None	Physically destroy the media so that the data cannot be recovered or reused, such as cutting into small pieces, drilling, crushing, or incineration.
2) **Magnetic Media** (e.g., Tape Backup)	None	
3) **Magnetic Media** (e.g., SATA Hard Disk, SCSI Hard Disk)	Overwrite existing data at least once (Format ⟶ Overwrite ⟶ Format)	
4) **Flash Memory Storage** (e.g., SSD, Flash Drive, Memory Card, NVMe)	Overwrite existing data at least once (Format ⟶ Overwrite ⟶ Format)	

4. Computer Usage Practices

4.1) General Practices

1) Computers shall be used solely for the Company's business operations. In addition, persons who are assigned computers shall endeavor to use such computers to support the Company's business operations. The use of computers for personal purposes or for any other activities unrelated to the Company's business is strictly prohibited.
2) The ICT Department shall determine appropriate access rights to information stored in computers in order to prevent data leakage or loss. In addition, computer users shall endeavor to prevent any data leakage or loss to the extent permitted by their access rights. Access to information beyond one's authorized rights is strictly prohibited.
3) The installation of programs that are not necessary for work performance is prohibited. The installation of unlicensed software is strictly prohibited, even if such software is required for work performance.

4) The installation of software that has been prohibited by the Company or the ICT Department is strictly prohibited.

5) No person shall modify or alter computer settings configured by the ICT Department without authorization.

6) The storage and maintenance of data in computers shall take into account the necessity of data backup in accordance with the level of importance of such data. Data should be backed up regularly. Critical data shall be backed up in the File Sharing Server. In this regard, the number of backups in backup media of the server and the storage location shall be determined and secured appropriately.

7) Mobile phones and smartphones used for work purposes shall be equipped with security measures such as dial lock or key lock, and antivirus software should be installed.

4.2) Security Measures

1) The ICT Department shall instruct all persons subject to this Policy regarding appropriate security measures and shall regularly monitor and verify compliance with such measures
2) Computers must be configured to automatically enable a forced lock screen after 15 minutes of inactivity (idle time)
3) The ERP system must be configured to automatically force log-out after 15 minutes of inactivity
4) Passwords for computer and ERP system access shall be subject to a password history policy of 365 days before reuse of a previous password is permitted
5) All computers and servers must have antivirus software installed, and the version, scan engine, and pattern files must be kept up to date at all times In addition, the antivirus software must be continuously active and configured to scan emails, file downloads, and file copy activities
6) In cases where a virus infection is suspected, persons subject to this Policy must disconnect the network cable immediately and report the incident to the ICT Department Full cooperation must be provided in identifying the cause and eliminating the virus
7) Security measures for operating systems and applications must be implemented for example, office computers must update Microsoft Windows on a weekly basis

8) Computers operating on operating systems for which vendor security support has expired shall not be connected to the Company's network
9) To prevent data loss, hard disk encryption should be implemented

4.3 Password Control Measures for Usage

1) Users who request to add, modify, or revoke access rights and receive approval at manager level or above via the IT Care system must carefully safeguard their passwords and comply with the following

- Passwords must not be shared or used jointly
- Passwords must not be easily guessable and must be at least 8 characters in length including a combination of numbers (0–9), uppercase letters (A–Z), lowercase letters (a–z), and special characters (such as # & ! @ $ % ^)
- Passwords must not be recorded in visible locations such as computer screens or desks If necessary they must be securely stored such as in a locked drawer
- Passwords must be changed every 90 days
- Users must ensure that passwords are not visible to others when being entered
- After 5 incorrect login attempts the account will be locked and a request must be submitted via the IT Care system for reset

2) Privileged passwords for operating systems including Windows and Unix/Linux shall expire every 90 days and must be stronger than general user passwords requiring at least 12 characters including numbers uppercase letters lowercase letters and special characters The ICT Manager shall be responsible for enforcement
3) ERP system script passwords embedded within programs which are not used for normal operations may be exempt from periodic changes where necessary in order to prevent disruption of system functionality as detailed in Appendix A ERP User Details
4) Passwords for service providers accessing systems via VPN upon approved request shall be valid for 48 hours per request and must comply with the same password requirements as general users
5) User access rights must be reviewed at least once annually

4.4 Use of Notebook Computers Outside the Company

1) Users must exercise due care to prevent loss theft or damage of notebook computers Any such incidents must be reported immediately to the ICT Department

2) The use of notebook computers outside the Company increases the risk of data leakage and virus infection Users must therefore exercise heightened security awareness including regular password changes maintaining antivirus protection not storing passwords on the device and increasing the frequency of Windows updates.

5. Network System

5.1) General Information

1) The ICT Department shall be responsible for maintaining the Company's network system in an appropriate manner
2) The ICT Department must monitor the usage of IP addresses for each user and implement strict controls to ensure user identification In this regard usage is prohibited if the IP address is not assigned by the DHCP Server
3) In cases where the Company's network is connected to external networks via WAN (Wide Area Network) the ICT Department must understand applicable information security policies and standards relating to network architecture and must strictly enforce compliance by all persons subject to this Policy
4) The network system shall not be used for purposes other than business operations
5) Users must use the network appropriately carefully and prudently to prevent data leakage
6) Under no circumstances shall any data obtained be used in any unlawful manner such as data theft
7) It is prohibited to connect any devices such as personal computers to the Company's network without prior authorization from the ICT Department
8) In the event that backup communication systems are unavailable it is prohibited to connect to external networks via dial-up or any other methods unless approved by the ICT Department as appropriate
9) Any actions that may reduce network security are prohibited such as the use of tunnel software
10) Any communication that imposes excessive load on the network such as online music streaming or viewing YouTube is prohibited
11) Packet monitoring or interception of data on the network is prohibited

12) Windows shared disk usage may be permitted within the scope approved by the ICT Department however sharing system drives such as C:\ is strictly prohibited
13) Transmission of files that may harm other devices such as files containing viruses is prohibited
14) Prohibited conduct related to the use of the Company's network system includes

- Copyright infringement such as unauthorized use of text images or data belonging to others including books magazines newspapers articles or web pages
- Trademark infringement such as unauthorized use of marks or symbols used to distinguish goods or services
- Image rights infringement such as unauthorized use or dissemination of photographs or images of other individuals
- Personal data infringement such as unauthorized use or disclosure of personal data including name surname address telephone number or identification number
- Defamation or actions that damage the reputation of others including dissemination of information that harms another company's reputation
- Distribution or publication of obscene or inappropriate content including posting of links

15) Mobile devices or tablets shall not be connected to the internal network unless prior approval is obtained from the ICT Department and required security controls such as antivirus and mobile device management (MDM) are installed
16) External visitors are not permitted to access the Company's internal network If necessary they may access the internet only via the Pinthong-Guest WiFi system subject to registration through the designated web portal with a usage period limited to 2 hours and re-registration required upon expiration

5.2 E-mail System

1) The ICT Department shall appropriately manage and control email users subject to ICT approval
2) Email shall not be used for purposes other than business operations
3) Passwords must be properly set and must not be stored in email programs and users must not use another person's user account
4) In cases involving the transmission of confidential information appropriate measures must be taken and due care must be exercised in sending such information

5) When replying to or forwarding emails consideration must be given as to whether the content contains confidential information
6) Proper email etiquette must be maintained for both internal and external communications
7) The maximum file size for email transmission shall be 130 MB and files exceeding this size cannot be sent
8) Files received from unknown or suspicious sources must be deleted immediately and no action shall be taken on such files
9) The ICT Department may monitor email transmission and receipt details without prior notice and persons subject to this Policy acknowledge such monitoring

5.3 Website System

1) The ICT Department shall appropriately manage web system users subject to approval from the ICT Manager
2) The web system shall not be used for purposes other than business operations
3) Passwords must be properly set and must not be stored in browsers and users must not use another person's user account
4) An appropriate proxy system must be used
5) Access to unsafe websites or advertisements is prohibited
6) Access to internal or external websites for purposes of harassment or any unlawful or improper intent is prohibited
7) Downloading files not necessary for business operations is prohibited Even if necessary files are downloaded they must not be executed directly from the browser and must be scanned for viruses prior to use
8) The ICT Department may monitor website access details without prior notice and persons subject to this Policy acknowledge such monitoring
9) Access to external websites that may capture or record Company data is prohibited
10) The ICT Department shall periodically monitor computer and network usage
11) The ICT Department shall implement system logs and access logs for monitoring access to information disclosed externally and shall periodically review such logs for potential threats or malicious activities

12) The ICT Department shall establish rules for vulnerability assessment relating to externally published content and shall conduct periodic reviews to ensure system integrity and prevent security vulnerabilities

6. Policy on Personal Data Management Stored in Computer Systems

6.1) Types of Data Collected

1) Personal Data shall mean any information relating to the identification of a natural person A natural person who is identifiable refers to an individual who can be identified directly or indirectly by reference to any identifier but does not include data of deceased persons in particular
2) System Data shall mean data collected when using the domains Pinthongindustrial.com and Pin-pure.com including technical data such as IP address browser type browsing history access time referring website and search information
3) Location Data shall mean data obtained from GPS WiFi compass IP address or public posts indicating location information
4) Website Cookies shall mean data placed on a computer by a web server After cookies are stored they will retain and remember user information until the browser is closed or until the user deletes or rejects the cookies Cookies facilitate easier website usage by storing visited website information
5) Other Data shall include images and or audio recordings from CCTV photographs audio visual recordings and voice recordings of conversations

6.2) Purpose of Personal Data Processing

1) Customer Personal Data

Customer personal data refers to personal data of customers excluding juristic persons where the primary data user and data process.or are the Sales Department and Accounting and Finance Department

1.1) To provide service information and organize activities

1.2) To provide support and maintenance related to real estate

1.3) To respond to inquiries and provide consultation

1.4) To issue service certificates under warranty

1.5) To provide membership services

1.6) To develop and improve real estate including conducting surveys and questionnaires for evaluation purposes

1.7) To provide information services and prepare statistical data

1.8) To conduct audits for the purpose of developing and improving business strategies or management policies

1.9) To perform contractual obligations

1.10) To conduct negotiations with customers in meetings

1.11) To provide useful information to customers of the Company

2) Personal Data Relating to Shareholders

Personal data relating to shareholders shall mean personal data of shareholders, where the primary data user and data processor are the Company Secretary or the Company Registrar

2.1) To perform rights and obligations in accordance with applicable laws and the Company's Articles of Association

2.2) To facilitate convenience in usage such as dividend statements to be received by shareholders

2.3) To implement shareholder-related measures such as questionnaires

2.4) To manage shareholder data in accordance with laws and regulations such as shareholder record creation

3) Personal Data Relating to Officers / Employees / Interns

Personal data relating to officers' employees and interns shall mean personal data of employee's job applicants and interns, where the primary data user and data processor are the Human Resources and Administration Department

3.1) To facilitate communication and negotiation for the Company's operations

3.2) To manage and process income payroll compensation and other benefits for officers' employees and interns

4) Personal Data Relating to Suppliers / Contractors

Personal data relating to suppliers or contractors shall mean personal data of such suppliers or contractors, where the primary data user and data processor are the Procurement Department and Accounting and Finance Department

4.1) To verify information qualifications and conduct procurement processes of the Company

4.2) To perform contractual obligations and assigned work

4.3) To process payments and perform accounting and financial operations

5) Personal Data Relating to Employment

Personal data relating to employment shall mean personal data of employees and job applicants, where the primary data user and data processor are the Human Resources and Administration Department

5.1) To be used for job application contact and recruitment consideration

5.2) To manage the Company's operations and related matters

5.3) To communicate with former employees

6) Other Data for the Security of the Company

Other data shall include, but not be limited to, images and/or audio recordings from closed-circuit television (CCTV), photographs, audio-visual recordings, and voice recordings of conversations, where the primary data user and data processor are the ICT Department and the Common Area Management Department

6.1) To monitor and review the use of the Company's services in order to improve security standards in service provision, management, and protection of information technology infrastructure

6.2) To control access to and from buildings and to ensure that the Company's buildings and premises are safe and secure for personnel, as well as for assets and data located or stored therein, including monitoring and surveillance of entry and exit to buildings, secured areas, restricted rooms, information technology infrastructure, operational data areas, and other designated areas (collectively referred to as "buildings and premises"), in order to prevent unauthorized access and to prevent, detect, and investigate security-related incidents such as unauthorized access, theft, fire, or physical harm.

6.3) Disclosure of Personal Data

The Company may disclose the aforementioned personal data under the specified purposes and in accordance with applicable legal requirements to the following entities and persons

(1) Pinthong Industrial Park Public Company Limited and the Pinthong Group including its employees staff directors managers or relevant personnel as necessary for personal data processing
(2) Government authorities and regulatory bodies as required by law
(3) Entities authorized by law to request disclosure of such information
(4) Business partners service providers contractors and data processors appointed by the Company to manage process or support personal data including but not limited to system development maintenance information technology security payment systems auditing and human resource management
(5) Disclosure of personal data to third parties excluding juristic persons shall be carried out only for the specified purposes or other purposes permitted by law Where consent is required by law the Company shall obtain explicit consent from the data subject prior to disclosure
(6) In cases where the Company discloses personal data to third parties the Company shall implement appropriate measures to protect such data and ensure compliance with applicable personal data protection laws

6.4) Consent and Data Subject Rights

The collection use or disclosure of personal data shall require consent from the data subject prior to or at the time of processing Consent shall be obtained in writing via forms or other methods as determined by the Company The data subject shall have the following rights

1) The right to access personal data and be informed of data collected
2) The right to rectify inaccurate incomplete or outdated personal data to ensure accuracy and currency
3) The right to request deletion of personal data where such data is no longer necessary for the purposes of processing or where consent has been withdrawn or where processing is unlawful

6.5) Data Retention Period

1) Personal data relating to employees and job applicants shall be retained throughout the period of employment
2) Personal data relating to suppliers or contractors shall be retained throughout the duration of the business relationship

3) Personal data relating to customers excluding juristic persons shall be retained throughout the duration of the business relationship

6.6) Compliance with Personal Data Management Policy

The implementation of this personal data management policy shall be in accordance with the Personal Data Protection Act B.E. 2562 (2019) and all relevant subordinate laws including any amendments in the future as well as the Company's Personal Data Protection Policy and Personal Data Management Guidelines (PDPA) of Pinthong Industrial Park Public Company Limited dated 25 February 2022 including any subsequent revisions or updates

7. Control of Service Providers for System Management

7.1) Selection of Service Providers

In cases where the Company engages a system service provider, such provider must be reliable and capable of performing duties in accordance with the defined scope of work

7.2) Contractual Agreement with Service Providers

Any contract or written agreement with a system service provider must include provisions relating to information security as follows

1) Strict compliance with the Company's information security policies
2) Confidentiality of information

- Disclosure or dissemination of any received information to third parties is prohibited without prior authorization from a supervisor or an authorized person

3) Proper data management

- Clear identification of responsible persons for data management such as the service provider's responsible manager
- Proper control and protection of data to prevent loss leakage or unauthorized modification
- In cases where storage media or devices are delivered such devices must be scanned for viruses prior to use

4) Penalties for non-compliance

- In cases of breach of contract appropriate measures shall be enforced such as claims for damages or other legal actions

7.3 Control of Service Provider Access

1) Service providers performing remote access for system maintenance improvement or troubleshooting must request prior approval and obtain VPN access credentials by submitting a request via email to the ICT Department for consideration as appropriate
2) Passwords used by service providers to log in and connect via VPN shall be valid for no more than 48 hours per request

8. Precautions Regarding Information Systems

Appropriate physical security measures shall be implemented, including

- The placement of server racks and establishment of a dedicated server room
- Emergency measures to address incidents such as earthquakes power outages fire air conditioning failures electrical systems and cabling arrangements
- Access control measures for the server room including restriction of access rights logging of entry and exit and periodic review of access logs

8.1) Core systems should be regularly backed up and backup results must be verified on a regular basis

8.2) File servers should maintain backups on more than one storage media to ensure availability in the event of data loss or damage

8.3) Mail System

- Email transmission and receipt logs shall be retained for at least 90 days
- Users should maintain email archives for at least 90 days

8.4) Proxy systems should retain logs of external website access for at least 90 days in accordance with legal requirements

9. User Account Control

9.1) Account Creation

Requests for user account creation must be submitted through the IT Care system for the ICT Department to process in accordance with the request The ICT Department must ensure that shared accounts are not created

9.2) Account Deletion

Requests for deletion of unused accounts must be submitted In cases of employee transfer

or resignation the ICT Department must verify supporting documentation from the Human Resources and Administration Department before deleting or disabling such accounts After deletion or deactivation the account must be retained for at least 90 days before permanent removal from the system

9.3) Account Modification

Requests for modification or changes to user account information must be submitted through the IT Care system for processing by the ICT Department

10. Handling of Unexpected Incidents

10.1) Incident Occurrence

In the event of any incident regardless of impact whether direct or indirect the ICT Department must record an Incident Report for every occurrence including details of corrective actions taken and analysis of root causes to prevent recurrence

10.2) Prevention of Recurrence

The ICT Department must analyze incidents and establish preventive measures to avoid recurrence

10.3) Emergency Response Plan

The Company shall conduct regular drills and review the Business Continuity Plan at least once per year to ensure preparedness and effective system recovery procedures

11. Others

11.1) Compliance with Laws

In addition to the rules and regulations set forth in this Policy, all persons subject to this Policy shall strictly comply with the laws of the Kingdom of Thailand and the Company’s internal regulations

11.2) Reporting

In the event of any incident that is inconsistent with or violates this Policy or where any conduct contrary to this Policy is observed, such incident must be reported immediately to the ICT Department

11.3) Monitoring and Review

The ICT Department shall establish a plan to monitor compliance with this Policy on a regular

basis and assess the appropriateness of this Policy including periodic review and revision as necessary

11.4) Penalties

In the event that any person subject to this Policy violates its provisions, the Company may consider suspension or termination of user accounts and may impose disciplinary actions in accordance with the Company's regulations as appropriate or pursue legal action where applicable

11.5) Compensation for Damages

In cases where any violation of this Policy results in significant damage to the Company whether intentional or unintentional the Company may require the responsible person to compensate for such damages

11.6) Education Training and Awareness

The ICT Department shall provide information technology knowledge to users of information assets including organizing training programs and maintaining training records such as training dates participant lists and training content or providing awareness through various channels such as email or computer screen background messages

11.7) Amendments

Any person wishing to propose amendments to this Policy must submit a request to the ICT Department for consideration This Policy shall be reviewed and updated at least once per yea

This Information Technology Security Policy Revision No. 6 shall be effective from 13 November 2024, by the approval of the Board of Directors at its Meeting No. 4/2024.

- Mr. Prasan Tanprasert -
Chairman of the Board of Directors
Pinthong Industrial Park Public Company Limited

Appendix A: ERP System Username Details

Linux ERPPROD และ ERPPRODDB

NO.	USER	Server	Password Policy
1	root	ERPPROD, ERPPRODDB	90 DAYS
2	sarunyou	ERPPROD, ERPPRODDB	90 DAYS
3	teerawit	ERPPROD, ERPPRODDB	90 DAYS
4	abrt	ERPPROD, ERPPRODDB	NO
5	adm	ERPPROD, ERPPRODDB	NO
6	applprod	ERPPROD, ERPPRODDB	NO
7	avahi	ERPPROD, ERPPRODDB	NO
8	avahi-autoipd	ERPPROD, ERPPRODDB	NO
9	bin	ERPPROD, ERPPRODDB	NO
10	chrony	ERPPROD, ERPPRODDB	NO
11	colord	ERPPROD, ERPPRODDB	NO
12	daemon	ERPPROD, ERPPRODDB	NO
13	dbus	ERPPROD, ERPPRODDB	NO

14	ftp	ERPPROD, ERPPRODDB	NO
15	games	ERPPROD, ERPPRODDB	NO
16	gdm	ERPPROD, ERPPRODDB	NO
17	geoclue	ERPPROD, ERPPRODDB	NO
18	gnome-initial-setup	ERPPROD, ERPPRODDB	NO
19	halt	ERPPROD, ERPPRODDB	NO
20	libstoragemgmt	ERPPROD, ERPPRODDB	NO
21	lp	ERPPROD, ERPPRODDB	NO
22	mail	ERPPROD, ERPPRODDB	NO
23	nfsnobody	ERPPROD, ERPPRODDB	NO
24	nobody	ERPPROD, ERPPRODDB	NO
25	ntp	ERPPROD, ERPPRODDB	NO
26	operator	ERPPROD, ERPPRODDB	NO
27	oracle	ERPPROD, ERPPRODDB	NO
28	polkitd	ERPPROD, ERPPRODDB	NO

29	postfix	ERPPROD, ERPPRODDB	NO
30	pulse	ERPPROD, ERPPRODDB	NO
31	qemu	ERPPROD, ERPPRODDB	NO
32	radvd	ERPPROD, ERPPRODDB	NO
33	rpc	ERPPROD, ERPPRODDB	NO
34	rpcuser	ERPPROD, ERPPRODDB	NO
35	rtkit	ERPPROD, ERPPRODDB	NO
36	saslauth	ERPPROD, ERPPRODDB	NO
37	setroubleshoot	ERPPROD, ERPPRODDB	NO
38	shutdown	ERPPROD, ERPPRODDB	NO
39	sshd	ERPPROD, ERPPRODDB	NO
40	sync	ERPPROD, ERPPRODDB	NO
41	systemd-bus-proxy	ERPPROD, ERPPRODDB	NO
42	systemd-network	ERPPROD, ERPPRODDB	NO
43	tcpdump	ERPPROD, ERPPRODDB	NO

44	tss	ERPPROD, ERPPRODDB	NO
45	unbound	ERPPROD, ERPPRODDB	NO
46	upload	ERPPROD	NO
47	usbmuxd	ERPPROD, ERPPRODDB	NO

ORACLE DB

NO.	USER	System	Password Policy
1	SYS	ORACLE DB	90 DAYS
2	SYSTEM	ORACLE DB	90 DAYS
3	AD_MONITOR	ORACLE DB	NO
4	AHL	ORACLE DB	NO
5	AK	ORACLE DB	NO
6	ALR	ORACLE DB	NO
7	AMS	ORACLE DB	NO
8	AMV	ORACLE DB	NO
9	ANONYMOUS	ORACLE DB	NO
10	AP	ORACLE DB	NO
11	APPLSYS	ORACLE DB	NO
12	APPLSYSPUB	ORACLE DB	NO
13	APPQOSSYS	ORACLE DB	NO
14	APPS	ORACLE DB	NO
15	APPS_NE	ORACLE DB	NO
16	AR	ORACLE DB	NO
17	ASF	ORACLE DB	NO
18	ASG	ORACLE DB	NO
19	ASL	ORACLE DB	NO
20	ASN	ORACLE DB	NO
21	ASO	ORACLE DB	NO
22	ASP	ORACLE DB	NO
23	AST	ORACLE DB	NO
24	AUDSYS	ORACLE DB	NO
25	AX	ORACLE DB	NO
26	AZ	ORACLE DB	NO
27	BEN	ORACLE DB	NO

28	BIC	ORACLE DB	NO
29	BIM	ORACLE DB	NO
30	BIS	ORACLE DB	NO
31	BNE	ORACLE DB	NO
32	BOM	ORACLE DB	NO
33	CCT	ORACLE DB	NO
34	CE	ORACLE DB	NO
35	CLA	ORACLE DB	NO
36	CLN	ORACLE DB	NO
37	CMI	ORACLE DB	NO
38	CN	ORACLE DB	NO
39	CRP	ORACLE DB	NO
40	CS	ORACLE DB	NO
41	CSC	ORACLE DB	NO
42	CSD	ORACLE DB	NO
43	CSE	ORACLE DB	NO
44	CSF	ORACLE DB	NO
45	CSI	ORACLE DB	NO
46	CSL	ORACLE DB	NO
47	CSM	ORACLE DB	NO
48	CSP	ORACLE DB	NO
49	CSR	ORACLE DB	NO
50	CTXSYS	ORACLE DB	NO
51	CUA	ORACLE DB	NO
52	CUG	ORACLE DB	NO
53	CZ	ORACLE DB	NO
54	DBSNMP	ORACLE DB	NO
55	DDR	ORACLE DB	NO
56	DIP	ORACLE DB	NO
57	DNA	ORACLE DB	NO

58	DOM	ORACLE DB	NO
59	DPP	ORACLE DB	NO
60	EAM	ORACLE DB	NO
61	EC	ORACLE DB	NO
62	ECX	ORACLE DB	NO
63	EDR	ORACLE DB	NO
64	EGO	ORACLE DB	NO
65	EM_MONITOR	ORACLE DB	NO
66	ENG	ORACLE DB	NO
67	ENI	ORACLE DB	NO
68	FA	ORACLE DB	NO
69	FLM	ORACLE DB	NO
70	FPA	ORACLE DB	NO
71	FRM	ORACLE DB	NO
72	FTE	ORACLE DB	NO
73	FUN	ORACLE DB	NO
74	FV	ORACLE DB	NO
75	GHG	ORACLE DB	NO
76	GL	ORACLE DB	NO
77	GMA	ORACLE DB	NO
78	GMD	ORACLE DB	NO
79	GME	ORACLE DB	NO
80	GMF	ORACLE DB	NO
81	GMI	ORACLE DB	NO
82	GML	ORACLE DB	NO
83	GMO	ORACLE DB	NO
84	GMP	ORACLE DB	NO
85	GMS	ORACLE DB	NO
86	GR	ORACLE DB	NO
87	GSMADMIN_INTERNAL	ORACLE DB	NO

88	GSMCATUSER	ORACLE DB	NO
89	GSMUSER	ORACLE DB	NO
90	HR	ORACLE DB	NO
91	HRI	ORACLE DB	NO
92	HXC	ORACLE DB	NO
93	HXT	ORACLE DB	NO
94	IA	ORACLE DB	NO
95	IBC	ORACLE DB	NO
96	IBE	ORACLE DB	NO
97	IBU	ORACLE DB	NO
98	IBW	ORACLE DB	NO
99	IBY	ORACLE DB	NO
100	ICX	ORACLE DB	NO
101	IEB	ORACLE DB	NO
102	IEC	ORACLE DB	NO
103	IEM	ORACLE DB	NO
104	IEO	ORACLE DB	NO
105	IES	ORACLE DB	NO
106	IEU	ORACLE DB	NO
107	IEX	ORACLE DB	NO
108	IGC	ORACLE DB	NO
109	IGI	ORACLE DB	NO
110	IMC	ORACLE DB	NO
111	INL	ORACLE DB	NO
112	INV	ORACLE DB	NO
113	IPA	ORACLE DB	NO
114	IPM	ORACLE DB	NO
115	ITG	ORACLE DB	NO
116	IZU	ORACLE DB	NO
117	JA	ORACLE DB	NO

118	JE	ORACLE DB	NO
119	JG	ORACLE DB	NO
120	JL	ORACLE DB	NO
121	JMF	ORACLE DB	NO
122	JTF	ORACLE DB	NO
123	JTM	ORACLE DB	NO
124	LNS	ORACLE DB	NO
125	MDDATA	ORACLE DB	NO
126	MDSYS	ORACLE DB	NO
127	MFG	ORACLE DB	NO
128	MGDSYS	ORACLE DB	NO
129	MRP	ORACLE DB	NO
130	MSC	ORACLE DB	NO
131	MSD	ORACLE DB	NO
132	MSO	ORACLE DB	NO
133	MSR	ORACLE DB	NO
134	MTH	ORACLE DB	NO
135	MWA	ORACLE DB	NO
136	ODM	ORACLE DB	NO
137	ODM_MTR	ORACLE DB	NO
138	OE	ORACLE DB	NO
139	OJVMSYS	ORACLE DB	NO
140	OKC	ORACLE DB	NO
141	OKE	ORACLE DB	NO
142	OKL	ORACLE DB	NO
143	OKS	ORACLE DB	NO
144	OKX	ORACLE DB	NO
145	OLAPSYS	ORACLE DB	NO
146	ONT	ORACLE DB	NO
147	OPI	ORACLE DB	NO

148	ORACLE_OCM	ORACLE DB	NO
149	ORDDATA	ORACLE DB	NO
150	ORDPLUGINS	ORACLE DB	NO
151	ORDSYS	ORACLE DB	NO
152	OSM	ORACLE DB	NO
153	OTA	ORACLE DB	NO
154	OUTLN	ORACLE DB	NO
155	OZF	ORACLE DB	NO
156	PA	ORACLE DB	NO
157	PJI	ORACLE DB	NO
158	PJM	ORACLE DB	NO
159	PMI	ORACLE DB	NO
160	PN	ORACLE DB	NO
161	PO	ORACLE DB	NO
162	POM	ORACLE DB	NO
163	PON	ORACLE DB	NO
164	POS	ORACLE DB	NO
165	PRP	ORACLE DB	NO
166	PSA	ORACLE DB	NO
167	PSP	ORACLE DB	NO
168	PV	ORACLE DB	NO
169	QA	ORACLE DB	NO
170	QOT	ORACLE DB	NO
171	QP	ORACLE DB	NO
172	QPR	ORACLE DB	NO
173	QRM	ORACLE DB	NO
174	RG	ORACLE DB	NO
175	RLM	ORACLE DB	NO
176	RRS	ORACLE DB	NO
177	SCOTT	ORACLE DB	NO

178	SI_INFORMTN_SCHEMA	ORACLE DB	NO
179	SPATIAL_CSW_ADMIN_USR	ORACLE DB	NO
180	SPATIAL_WFS_ADMIN_USR	ORACLE DB	NO
181	SSOSDK	ORACLE DB	NO
182	SSP	ORACLE DB	NO
183	SYSBACKUP	ORACLE DB	NO
184	SYSDG	ORACLE DB	NO
185	SYSKM	ORACLE DB	NO
186	TEERAWIT	ORACLE DB	NO
187	VEA	ORACLE DB	NO
188	WIP	ORACLE DB	NO
189	WMS	ORACLE DB	NO
190	WPS	ORACLE DB	NO
191	WSH	ORACLE DB	NO
192	WSM	ORACLE DB	NO
193	XCUST	ORACLE DB	NO
194	XDB	ORACLE DB	NO
195	XDO	ORACLE DB	NO
196	XDP	ORACLE DB	NO
197	XLA	ORACLE DB	NO
198	XLE	ORACLE DB	NO
199	XNB	ORACLE DB	NO
200	XNP	ORACLE DB	NO
201	XPN	ORACLE DB	NO
202	XS$NULL	ORACLE DB	NO
203	XTR	ORACLE DB	NO
204	YMS	ORACLE DB	NO
205	ZX	ORACLE DB	NO