REGULATIONS FOR THE SECURITY OF INTERNET BANKING

PAYMENT SYSTEMS DEPARTMENT

STATE BANK OF PAKISTAN

Table of Contents

PREFACE

Internet Banking has become an important delivery channel for banking services enabling banks to offer traditional banking services like access to one or multiple accounts for fund transfers, bill payments and card payments etc through internet. The security of Internet Banking has become a major concern for the regulatory authorities because of increasing IT security risks which may lead to serious financial and reputation risks in case of any major security breach. These regulations, therefore, would help banks in Pakistan to develop a formal Internet Banking Security Framework containing administrative, technical and physical safeguards based on best international practices. The major components of the framework would be Security Risk Assessment (of threats, vulnerabilities to systems and customers information), Security Controls Implementation based on the Security Risk Assessment and Security Controls Monitoring. An effective customer awareness program is also necessary to mitigate the risks associated with Internet Banking. Banks, therefore, are encouraged to regularly update their customers about the identity theft and fraud techniques, enabling them to identify these techniques and take appropriate preventive measures.

DEFINITIONS

Access Device: means any device used by customers to access Internet Banking services.

Customer: means a person that is maintaining an account with a bank and using Internet Banking to access that account.

Encryption: is a process of encoding information or data into a form called cipher-text, so that only authorized parties can read it.

Identity Theft Prevention: is an arrangement developed and implemented in order to identify, prevent and mitigate identity thefts in compliance with these regulations.

Internet Banking: for the purpose of these regulations means electronic delivery of banking products and services like accessing accounts for fund transfers, utility bill payments and obtaining financial information, by the customers through internet irrespective of the access device used.

Intrusion Detection System (IDS): means network security applications\appliances which monitor events occurring in a computer system or network in order to identify violations, malicious activity and suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Intrusion Prevention System (IPS): is an extension of IDS, which in addition to performing intrusion detection also attempts to stop possible incidents.

Least Privilege Principle: The principle that security architecture should be designed in a way that each entity is granted the minimum system resources and authorizations needed by the entity to perform its functions.

Security Breach: is any incident that results in unauthorized access of systems, applications, data, services, networks and/or devices by bypassing their underlying security mechanisms.

Security Controls: are formal arrangements made to avoid, counteract and minimize security risks identified by the bank in its Security Risk Assessment exercise. These include preventive, detective and corrective arrangements to mitigate security risks to protect bank’s assets.

Security Objectives: Series of statements that describe bank’s intent to safeguard itself from internal or external threats. Security objectives for Internet Banking primarily consist of confidentiality of information, integrity and availability of systems.

Security Framework: means documentation of management's decision that describes the detailed arrangements made for the protection of bank's customers, IT and communication resources. Security framework contains operational, administrative, technical and physical safeguards to meet the security objectives outlined by the bank.

Security Risk Assessment: is the process of identifying, estimating and prioritizing internet security risks to which bank's assets (customers, IT and communication resources) are exposed.

Service Providers (SPs): mean entities engaged by the bank for providing Internet Banking related products and services. This may include but is not limited to applications, hardware, communication, hosting, security, monitoring, systems development and maintenance, digital certification services, and call centers that support banks' Internet Banking related services.

Threats: are circumstances/events with the potential to adversely impact the operations of the bank and its assets.

Traceability: means the ability to discover information related to an event happened in a system by chronologically recording all related events in an unbroken manner to uniquely identify parties involved in a verifiable way.

Vulnerabilities: are the weaknesses in a system, or control gaps, if exploited, could result in the unauthorized disclosure, misuse, alteration, or destruction of information or information systems.

1. SCOPE OF THE REGULATIONS

These regulations are applicable to all banks in Pakistan providing financial and/or non financial transactions through internet irrespective of software tool used by the bank and access devices used by its customers.

2. INTERNET BANKING SECURITY FRAMEWORK

Bank shall develop, implement and regularly review Internet Banking Security Framework based on the following key security objectives:

a) Security and integrity of data and systems, to ensure that customers' information has not been modified and systems are free from unauthorized access;
b) Confidentiality of customers' data in storage, during processing and in transit;
c) Reliability and availability of Internet Banking systems to provide prompt access to systems for registered users and maintaining operational effectiveness;
d) Accountability by designing SOPs, policies and controls to ensure traceability of all transactions;
e) Proactive approach to detect unauthorized access and identification of potential fraudulent transactions.

While developing the Internet Banking Security Framework the bank should take into account the complexity of systems, applications and products /services offered while at the same time ensuring the ease of usage and customers' convenience. Further the framework should clearly define the roles and responsibilities of Board of Directors (BODs), senior management and employees with regard to its approval, development and implementation. This Framework and any reviews thereafter should be duly approved by the BODs.

The Internet Banking Security Framework shall include the following components:

- Security Risk Assessment
- Implementation of Security Controls and
- Monitoring of Security Controls

2.1. Security Risk Assessment

The bank shall conduct and document a formal Security Risk Assessment for Internet Banking with a view of identifying, estimating and prioritizing risks to which its operations are exposed due to Internet Banking. The BODs should review the risk assessment document and any reviews conducted thereafter.

The risk assessment shall cover at least the following aspects:

a) A current and detailed description of bank’s business and technology environment and existing security measures in place including identification of location, systems and methods for maintaining customers’ information;
b) An identification of information and the information systems to be protected;
c) Classification and ranking (high, medium, low) of the sensitive systems, payment data and applications in order of their importance and based on the assessment of threats and vulnerabilities;
d) Assessment of potential threats and vulnerabilities to security and integrity of customers’ information, payments data, IT systems and applications;
e) Assessment of risks related to identity theft and identity fraud;
f) An evaluation of existing Security Controls’ effectiveness against each threat and vulnerability;
g) The security and contractual responsibilities of Service Providers (SPs), including customers who have access to the bank’s systems and data;
h) Risks like Compliance, Concentration, Operational, Country and Legal should be assessed by the banks before entering and while managing Internet Banking outsourcing arrangements with the SPs;
i) Risk Assessment related to legal environment and bank’s responsibilities under Section 32 (Availability of Documentation and Proof), section 41 (Burden of Proof), Section 43 (Liability of banks/ Authorized Parties), section 70 (Secrecy and Privacy) and other relevant provisions of the Payment Systems and Electronic Fund Transfers Act 2007.

The Security Risk Assessment should be reviewed at least once a year; however, in case of a major security breach, significant changes to the infrastructure and introduction of a new product or service, an immediate review of risk assessment should be carried out. Further, in case of a major security breach, risk assessment review should include a detailed analysis of the factors that cause such security breaches.

2.2. Security Controls Implementation

The bank shall ensure that appropriate security arrangements and security controls to protect IT assets (such as systems, applications, networks, data, and information and communication systems) are in place. Bank shall develop a set of controls based on the Security Risk Assessment document, commensurate with the risk levels to meet the control objectives.

Bank shall define its set of minimum baseline Security Controls that include Access Controls (Access Rights Management, Electronic Authentication etc), Network Access Controls, Operating System Access Controls, Application Access and Remote

Access Controls. Minimum Security Controls to be implemented by banks should include the following aspects:

2.2.1. <u>Authentication Controls</u>

a) Registration/enrollment for Internet Banking customers should be done prior to offering Internet Banking products and services after due verification through appropriate means;

b) In order to authenticate customers who use Internet Banking products and services the bank shall implement at least Two Factor Authentication (2FA) such as Passwords (1 factor) and One time tokens, Dongles etc (2nd factor).

c) Bank shall implement additional layered security programs for high value transactions processed through Internet Banking;

d) Authentication controls should also take into account failed log-in attempts, frequency of password changes, session time outs and re-authentication of customers based on predefined criteria;

e) Bank shall conduct periodic risk assessment of authentication controls to identify threats and vulnerabilities based on changes in applications' functionality, threats due to changes in internal and external environment, changes in customers' preferences and actual security breaches;

2.2.2. <u>Security Controls for In-house Functions</u>

The following controls shall apply on bank employees who are users of Internet Banking related systems:

a) **Access Rights Management:** Users' access rights should be appropriate and commensurate with their job functions and should be periodically reviewed keeping in view the risk ranking of the systems, data and applications as outlined in Security Risk Assessment document. Changes in Access Rights should be based on personal or systems change and should only be applied after due authorization while ensuring proper implementation of "Least Privilege Principle".

b) **Operating Systems Controls:** Necessary Operating Systems' controls should be implemented to ensure that access is physically and logically secured by ensuring that privileged access is restricted, regularly monitored and periodically audited.

c) **Remote Access:** Remote access to high risk IT assets shall only be granted after management's approval in writing and should be subject to regular audits. Remote access shall also be based on strong authentication and encryption to secure communications.

d) **Physical Access:** Banks shall ensure that physical access to different systems, segments and data sites is restricted, regularly monitored and duly logged.

e) **IT Network Security:** IT networks shall be secured through the use of multiple layers of controls.

f) **Firewalls:** Firewalls shall be deployed between different security domains to control network traffic**.** Firewalls selection and deployment policy should be devised according to the characteristics of network (i.e. traffic volume, and risk classification of IT assets).

g) **IDS/IPS:** Network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) should be deployed between different security domains as per their risk classification.

h) **Identity Theft Prevention:** Bank shall develop and implement a proactive Identity Theft Prevention Program which includes procedures for identification of information to be protected, and threats due to thefts and frauds as well as methods for responding appropriately to identified threats.

i) **Encryption:** Access, storage and data communication shall be encrypted using reliable encryption methods to strengthen the security of communications and sensitive payment data.

j) **Traceability:** Bank shall maintain the traceability of transactions executed to discharge their obligations under the relevant sections of Payment Systems and Electronic Fund Transfers Act 2007.

k) **Training:** Relevant employees of the bank shall have appropriate knowledge and background to perform their tasks. Regular trainings should be arranged to keep employees aware of the security risks, security controls and security control monitoring mechanisms. Employees should be regularly updated about the changes in internal policies and procedures to ensure operational effectiveness.

2.2.3. Security Controls Implementation for Outsourced Functions

Service Providers of outsourced functions relating to Internet Banking are contractually bounded to implement these regulations. However, outsourcing does not relieve the bank from its responsibility of complying with these regulations. Further bank shall ensure that in addition to security controls mentioned in section 2.2.2, the following security controls for outsourced functions are also followed:

a) Contracts with Service Providers should be equipped with provision relating to Non Disclosure to ensure the confidentiality and security of bank and customers' information and to bank's as well as SBP's right to audit Service Providers' security controls as per the requirements set forth in these regulations;

b) Appropriate measures to avoid any loss, theft or leakage of customers' information are developed and implemented by the Service Providers;

c) Service Providers’ access to customer information is based on the request from the bank or the concerned customer and should be strictly monitored, logged and periodically audited. Further, customer information shall not be transferred to unauthorized storage or access medium.

d) Service Providers shall also have:

   i. A Disaster Recovery (DR) plan and its alignment with bank’s business requirements.
   ii. Different types of Disaster Recovery (DR) Sites: Cold / Warm / Hot / Satellite.
   iii. Documentation related to IT assets life cycle management.

2.3. <u>Security Controls Monitoring</u>

Bank shall develop and implement a formally approved mechanism for the monitoring of Security Controls. An analysis of the effectiveness of existing or proposed Security Controls Monitoring methods shall be part of this monitoring mechanism. Bank shall ensure that the following aspects are covered in the Security Controls Monitoring mechanism:

a) Monitoring of bank’s network activity by collecting and analyzing the host and network data related to security events. Examples of security events include privileged access to sensitive operating systems, configuration changes, and access to critical applications etc;

b) Methods for proactive monitoring of IDS/IPS and for responding to security breaches should be listed in detail in the monitoring mechanism. A rapid response team should be nominated and made responsible to respond immediately in case of a security breach;

c) Monitoring and reporting mechanism of Authentication Controls should be formally documented and approved by the senior management and implemented accordingly;

d) Procedures and time required for restoration of bank’s systems should be part of Security Controls Monitoring process;

e) Use of self-assessments, penetration testing, and independent security audits commensurate with the systems’ complexity and risk exposures;

f) Identification and listing of bank’s policy violations, unauthorized configuration changes and other conditions which can potentially increase the risk of security breaches;

g) Procedures to ensure the monitoring of logs and audit trails on regular and pre-defined periodic basis should be developed. The security logs and audit trials for IB should be retained for a period of ten years.

3. CUSTOMER AWARENESS

A formal customer awareness program regarding Internet Banking threats and safeguards to minimize frauds and Identity Theft risks should be developed and implemented by the banks.

This program should cover the following aspects:

a) An explanation of liabilities, roles and responsibilities of bank as well as its customers for using Internet Banking products and services offered by the bank;

b) Compliance of Disclosure requirements under Section 30 (Terms and Conditions of Transfers) of Payment Systems and Electronic Fund Transfer Act 2007;

c) Contact details of help desk that customer might need in case of any issues including loss of security credentials or frauds and identity theft;

d) Procedure for re-authentication of customers Internet Banking;

e) Complaint handling process including dispute resolution mechanism related to Internet Banking;

f) Regular issuance of guidelines to customers on yearly basis for mitigating the risks associated with Internet Banking;

g) Regular review and evaluation of the customer awareness programs by the management.

4. REPORTING REQUIREMENTS

All established security breaches should be reported to Payment Systems Department, State Bank of Pakistan. The incident and analysis reports of security breaches should be furnished on quarterly basis to PSD as per Annexure-I. Impact of security breach on institution’s business, systems, applications and customers should also be submitted in detail.

5. REGULATORY REQUIREMENTS

These regulations are subject to all relevant laws, rules and regulations issued by SBP from time-to-time including but not limited to the following:

a) Guidelines on the Outsourcing Arrangements (BPRD Circular No 9 dated July 13, 2007);

b) Guidelines on the Information Technology Security (BSD Circular No 15 dated September 29, 2004);

c) Information Systems: Guidelines on Audits and System Switchover Planning (BSD Circular No 8 dated December 12, 2005);

d) Compliance of “Guidelines on Business Continuity Planning” (BSD Circular No 13 dated September 04, 2004).

****

Annexure-I

Details of Established Security Breaches in IB

Name of the bank: ____________________ **For the Quarter Ending: ________________________**

Sr.	Source of security breach discovery	Nature of security breach	Reasons for the occurrence of security breach (e.g. Breach of controls, Procedures were not followed, weaknesses in implemented security controls etc.)	Impact of security breach (e.g. on banks business, systems, customers etc)	Action(s) taken to rectify the Security Breaches	Remarks (further details, if any)

Submitted By: ……..………(Name) ………..…….

Designation & Seal: ……………………………………….

Contact No: ……………………………………….