Reward Gateway Incident Management Policy

Classification – Confidential

November 2018 – Version 2.3

Reward Gateway
the employee engagement people

265 Tottenham Court Road
London
W1T 7RQ
UK

Table of contents

Document purpose

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident. The sections of this policy are built around the requirements of the ISO 27001 security standards.

The definition of an 'Information Security Incident' is an adverse event that has caused or has the potential to cause damage to Reward Gateway's assets, reputation and/or personnel. Incident Management is concerned with intrusion, compromise, and misuse of information and information resources, and the continuity of critical information systems and processes.

This policy aims to mitigate the following risks:

- To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
- To help identify areas for improvement to decrease the risk and impact of future incidents.

Scope

This policy applies to all users. The definition of users within this policy is intended to include every department, partner, employee of Reward Gateway, contractual third party, and agent who has access to organisation's IT systems or Data.

All users must understand and adopt the use of this policy. They are responsible for ensuring the safety and security of Reward Gateway's systems and the information they use or manipulate.

Roles

The Reward Gateway security incident response team is comprised of:

Role	Responsibility	Name	Email
Information Security Team	Incident Response Process Owners	Adam Altounyan Asen Varsanov	adam.altounyan@rewardgateway.com asen.varsanov@rewardgateway.com
Chief Technical Architect	Incident Response Technical Lead	William Tracz	will.tracz@rewardgateway.com

PR Manager	Handling of any external communications in relation to an incident	Charlie Lofthouse	charlie.lofthouse@rewardgateway.com
Primary HR contact	Handling of any personnel and disciplinary issues relating to security incidents	Robert Hicks	robert.hicks@rewardgateway.com
Head of Development	Security Incident Response Team Member	Hristo Mitev	hristo.mitev@rewardgateway.com
Primary DevOps contact	Security Incident Response Team Member	Miguel Arranz	miguel.arranz@rewardgateway.com
Group Director of Product & Client Success in Client Service	Security Incident Response Team Member	Robert Boland	rob.boland@rewardgateway.com

Responsibilities

The Incident Response Process Owners are responsible for:

- Making sure that the associated Security Incident reporting and response procedures and escalation procedures are defined and documented. This will help to make sure that the handling of any security incident is timely and effective.
- Making sure that the Security Incident Response Plan is up-to-date, reviewed and tested at least once every year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained, at least once every year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when it is needed.
- Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc.

- Authorising on-site investigations for law enforcement or payment card industry security/forensic personnel, as it is needed during any security incident investigation.

Security Incident Response Team members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the incident response lead of an incident when they received a security incident report from staff.
- Investigating each reported incident.
- Taking action to limit the exposure of sensitive or payment card data to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analysing logs and any related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Reporting each security incident and findings to the appropriate parties. This may include acquirer, card brands, third party service providers, business partners, customers.
- Assisting law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
- Resolving each incident to the satisfaction of all parties, including any external parties.
- Initiating follow-up actions to reduce the likelihood of recurrence, as is appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All employees are responsible for:

- Making sure that they understand how to identify and report a suspected or actual security incident
- Reporting a suspected or actual security incident through one of the formal methods described in this policy.
- Complying with the security policies and procedures of Reward Gateway. This includes any updated or temporary measures that are introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent a recurrence of an incident).

Incident definition

Events and weaknesses must be reported at the earliest possible stage. This is because they need to be assessed by the Head of Information Security in Security in

order to identify when a series of events or weaknesses have escalated to become an incident. It is vital the Head of Information Security in Security gains as much information as possible from the business users to identify if an incident is occurring.

Examples of the most common Information Security Incidents are listed in the table below. It should be noted that this list is not exhaustive.

Event Type	Examples
Malicious	• Giving information to someone who should not have access to it – verbally, in writing or electronically. • Computer infected by a Virus or other malware. • Receiving unsolicited mail which requires you to enter personal data. • Finding data that has been changed by an unauthorised person. • Receiving and forwarding chain letters – including virus warnings, scam warnings, and other emails which encourage the recipient to forward onto others. • Unknown people asking for information which could give them access to Reward Gateway data.
Misuse	• Deliberate or accidental actions that are in breach of Reward Gateway's security policies and procedures • Use of unapproved or unlicensed software on Reward Gateway equipment. • Use of unapproved or unlicensed software on Reward Gateway equipment. • Accessing a Reward Gateway IT resource using someone else's identity – e.g. someone else's user id and password. • Sending Personal Data in an e-mail. • Writing down your password and leaving it on display / somewhere easy to find – or any other violation over our Clear Desk and Clear Screen Policy. • Printing or copying confidential information and not storing it correctly or confidentially.
Theft / Loss	• Theft / loss of a hard copy document containing confidential or strictly confidential data. • Theft / loss of any Reward Gateway asset – access card, computer equipment, mobile phone, removable media. • Theft / loss of own device which contains company data – phone, computer, removable media.

Reward Gateway uses JIRA software for incident management. JIRA provides comprehensive classification for each event that has been logged. The classification groups are aligned with the control groups in the ISO 27002 security standard.

During the evaluation, the Head of Information Security in Security may refer to the metrics based on the impact over the Confidentiality, Integrity, and Availability as described in the Risk Assessment plan.

Incident priority

Agreeing and allocating on the appropriate priority is an important aspect of logging every incident as this will determine how the incident is handled and which procedures should be followed. The priority is based on on the *urgency* of the incident and the level of *impact* being caused to identify the required timelines for actions. The table below shows how this should be done:

		Impact		
Urgency	**Priority / Response time**	**High**	**Medium**	**Low**
	High	1 / 4 hours	2 / 24 hours	3 / 48 hours
	Medium	2 / 24 hours	3 / 48 hours	4 / 72 hours
	Low	3 / 48 hours	4 / 72 hours	5 / Planned

Timescales for incident response are based on the priority of the incident and must be aligned with the existing SLAs committed to by Reward Gateway.

'Response time' is the time between ticket transition from *Open* to *In Progress* status.

A separate procedure with greater urgency is followed for incidents defined as **Major**. Examples of Major incidents include:

- An incident that involves Strictly Confidential data (e.g. PCI or Personal Data).
- An incident which impacts the confidentiality, integrity or availability of the highest valued ISMS assets.
- Any security incident that could have a severe or catastrophic adverse effect on organisational operations, individuals, or clients.

Reporting procedure

During this process, it is vital for the Head of Information Security in Security to gain as much information as possible from the business users to identify if an incident is occurring, as well as the severity of it.

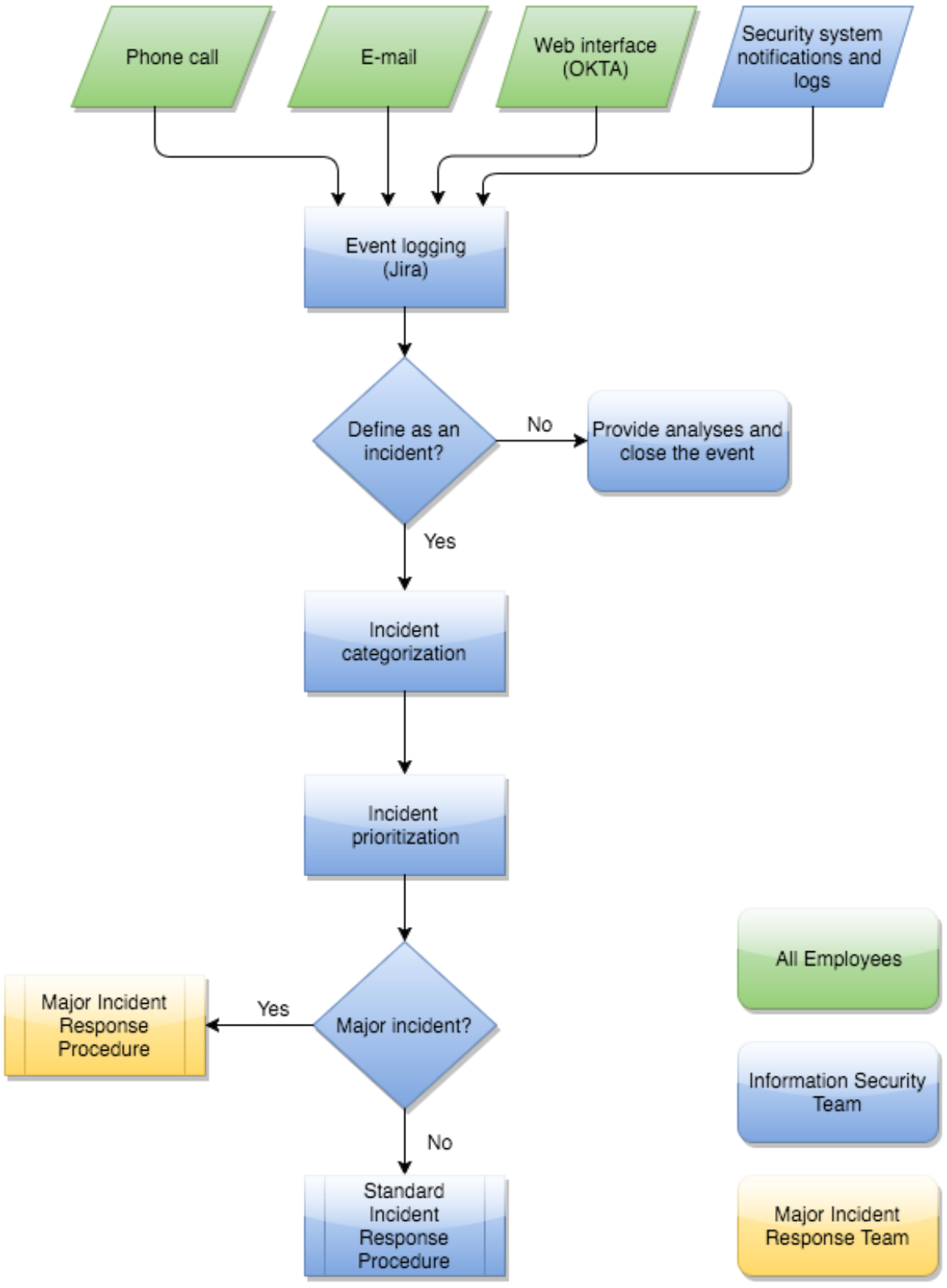
Reporting an event or security incident

If there is doubt whether an incident has occurred or not, it is strongly advised all users report immediately and let the Information Security Team know. The event must be reported at the earliest possible stage. The following communication channels for event reporting are available at Reward Gateway:

- Web interface – through the *Information Security Event Log* application available in OKTA
- E-mail at infosec@rewardgateway.com
- #infosec channel in Slack
- Automatically generated events reported by automated security systems (SIEM/DLP/Tenable.io/BlackDuck)
- Phone call - only in case of emergency and outside working hours

Regardless of the reporting method events must be registered in JIRA and further managed from within. After the initial report, if required, the employee may be asked to complete a Detailed Incident Report Form. The event reporting and handling procedure is shown on the diagram below.

Event reporting and handling procedure diagram



Reporting a security weakness

Security weaknesses must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered as misuse.

Examples of security weakness are:

- Poorly configured firewall
- Out-of-date anti-virus software
- System overload or malfunctioning
- Low resolution CCTV which does not allow face recognition
- Weak lock mechanism on a file cabinet holding sensitive information

Software bugs related to the Reward Gateway application are reported through the Service Desk.

Response procedure

The Information Security Team is responsible for the security event assessment, the execution of relevant procedures, and tracking the activities during the event life cycle. The response procedure is a post-reporting activity which presumes that the event is already reported and registered in JIRA.

Initial response and assessment

The assessment of security events plays a crucial part in their life cycle. During that stage, the Information Security Team must decide whether an incident occurred or if there is potential for the event to become a security incident in future. Depending on the result, the team must determine the most appropriate follow up response procedure.

1) Notify the internal/external parties with appropriate knowledge and permissions to manage systems or resources related to the event. Channel partners can be involved to cooperate on access issues. A contact list can be found in Section 20 of the ISMS Manual.
2) Verify the event confirming if the compromise is genuine or could lead to an incident:
    a) Classify the incident in category.
    b) Set a priority based on the criticality of the systems or data involved from a value of 1 through 5.

3) If the event is classified as an incident:
    a) Incidents with a priority of 2 through 5 will be remediated through the ***Standard Incident Response Procedure***.
    b) Incidents with priority value 1 are considered Major and follow the ***Major Incident Response Procedure***.
4) If the event is defined as false-positive and there is no reasonable belief that it could lead to an incident, provide analysis and close the event.

Standard incident response procedure

The standard incident response procedure is a seamless continuation of the initial response and assessment process. It is as follows:

1) Minimise further loss or damage – i.e. disable service, disconnect a system from the network, disable account.
2) Corrective action to repair and prevent reoccurrence – i.e. install patches, run anti-virus software.
3) Recover to normal operations.
4) Incident analysis and reporting:
    a) Determine the impact and cost of the damage, and the result of the attack.
    b) Generate an attack timeline and ascertain the attacker's actions.
5) Evaluate performance of the incident response plan and point out areas of improvement.

Only identified and authorised users should have access to the affected systems during the incident and all remedial actions must be documented. During the execution of this procedure, any evidence that might be required for later analysis must be collected and preserved.

Major incident response procedure

Major incident is everything that could have an extreme impact to Reward Gateway's business, such as excessive disruption of service or a breach of Personal or PCI Data. Data breach is an event where strictly confidential data in readable format (unencrypted) is being copied, transmitted, stolen or used by unauthorised party. The definition of strictly confidential data can be found in the ISMS Manual.

Major incidents may require activation of the appropriate Business Continuity Plan (BCP) during the recovery to normal service operation. These will be defined as **Priority 1** and the response will be instant.

In the earliest possible stage, a Major Incident Response Team must be formed to carry out the activities defined in the procedure below. Key staff members attending to resolution of major incidents are selected on an ad-hoc basis depending on the case. The Major Incident Response Team has the following participants:

- Chief Technical Architect – mandatory member.
- Head of Information Security in Security – mandatory member.
- Information Security Consultant – mandatory member.
- DevOps Engineer – if required.
- Head of Employee Support Team – if required.
- Head of Client Support Team – if required.
- Head of HR – if required.
- Head of Operations – if required.
- Every employee who has been involved or can assist for the successful resolution of the incident.

The following procedure is a continuation of the initial response and assessment process:

1) Minimize further loss or damage (i.e. disable service; disconnect a system from the network; disable account)
2) Perform initial investigation
    a) The Major Incident Response Team will investigate the incident and initiate actions to limit the exposure of payment card/personal data and in mitigating the risks associated with the incident.
    b) The Major Incident Response Team will determine if the third party had privileges to access the data or was the data encrypted in a way that would have prevented reading.
3) Notification (in case Personal or CHD data is involved)
    a) Notify affected data subjects taking into account the specific country legal requirements.
    b) Notify the relevant law enforcements depending on the market of operation and citizenship of affected data subjects.
    c) If PCI data has been involved then Reward Gateway's acquirer must be notified.
    d) Notify affected customers.
4) Action to repair and prevent recurrence (i.e. install patches; run anti-virus software)
5) Recover of operations and analysis (tasks are performed in parallel):
    a) Plan actions to restore the systems to normal operations and assign team members responsible for its execution

b) Perform in-depth investigation of the collected evidences
c) Create Detailed Incident Report (include incident timeline, root cause analyses, mechanisms for prevention, involved parties and data subjects, evaluate the impact and cost of damage).

6) Evaluate the performance of incident response plan and point out areas of improvement.

All major incidents must be escalated on hierarchical and functional level as required. The response team must decide if execution of appropriate BCP is required.

PCI DSS

Each payment card brand has specific requirements for reporting and responding to suspected or confirmed breaches of payment card data. As a merchant the primary contact if an incident occurs in Reward Gateway is our acquirer – HSBC.

Collection of evidence

Sources

To be considered in a court of law, all evidence being collected must be admissible. Reward Gateway has several sources which can be used in the collection process, though some are not relevant for each case:

- CCTV records
- Access logs to premises requiring key fobs
- Firewall logs
- Application logs
- Database logs
- Server logs
- Visitor Book records
- Screen snapshots
- Any objects that may contain fingerprints or DNA of the suspect
- Witness testimony

Collection and identification

Evidence should be protected through its life cycle, with the following information kept in an evidence log – a.k.a. chain of custody:

- Persons involved

- Description of evidence
- Location of evidence
- Date & Time
- Methods used – how evidence is discovered, collected and stored

The evidence must be marked without damage, with the collecting individual's initials, date, and case number. An evidence tag can be used if cannot be marked.

Preservation of evidence

All evidence must be properly stored in a secure facility and preserved to prevent damage or contamination from various hazards – including intense heat or cold, extreme humidity, water, magnetic fields, and vibration. Evidence which isn't properly protected may be inadmissible in court and the party responsible for the collection and its storage may be liable. Care must also be exercised during transportation to ensure that evidence is not lost, temporarily misplaced, damaged, or destroyed.

Learning from Information Security incidents

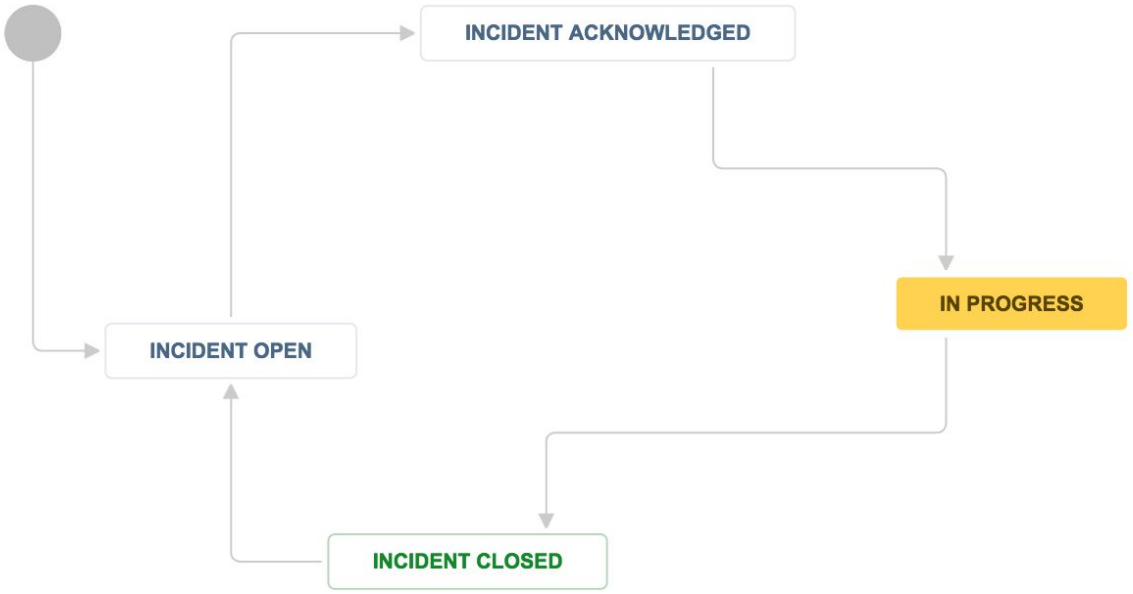
To learn from incidents and improve the response process, incidents must be recorded and a Post-Incident Review conducted. The following details must be retained:

- Incident Type – categorisation method based on control groups as defined in ISO 27002.
- Volume of incidents and priority levels – priority is based on 'impact' and 'urgency'.
- Incident location - system name or physical location.

The information must be collated and reviewed on a regular basis by the Head of Information Security in Security with any patterns and trends identified. If a significant trend has been observed, the Head of Information Security in Security must inform the Leadership Team and address appropriate actions to mitigate the risk.

Incident lifecycle diagram

The below diagram shows the incident management process integrated into JIRA.



Event lifecycle diagram

The below diagram shows the event management process integrated into JIRA.

External Contacts

External Party	Contact Name (if known)	Email	Telephone
HSBC (acquirer)	Matthew Garratt	matthew1.garratt@hsbc.com	-
UK National Fraud & Cyber Crime Reporting Centre		Report online: http://www.actionfraud.police.uk/report-a-fraud-including-online-crime-questions	0300 123 2040
In case the acquirer could not be reached:			
Visa Europe Data Compromise Team	-	datacompromise@visa.com	+44 (0) 20 7795 5031
MasterCard	-	account_data_compromise@mastercard.com	-
For reporting of breaches of Personal Data:			
UK Information Commissioner's Office (ICO)	-	casework@ico.gsi.gov.uk	Helpline: 0303 123 1113 Or 01625 545745

Revision history

Rev	Date	Author	Description	Approved	Date
1.0	13.07.2015	Ivan Dichev	First version	Richard Hurd-Wood	20.08.2015
2.0	14.04.2016	Ivan Dichev	Update on response procedures	Richard Hurd-Wood	25.04.2016
2.1	25.10.2016	Will Tracz	Detail on audit clarified.		
2.2	01.03.2017	Liam Jones Ivan Dichev	• Rebrand and general clean. • Update on PCI DSS incident management procedures.	Will Tracz	03.03.2017
2.3	26.11.2018	Asen Varsnaov	Update and review. Added Event lifecycle diagram.	Will Tracz	27.11.2018