Incident Response Plan

Version: 1.0

This version issued: 21/06/20

Date approved: 21/06/20

Date for review: 21/6/21

Owner: Matt Francis, Chief Information Officer

PURPOSE

Procreation UK Limited and the brand names it operates under, namely Cloudpresenter, Hubbub Wireless, BeatCast and Gravity Filming, collects information required for users to access its WebApps, webinars, video meetings, live streams, diary booking services and WiFi services. Information, like any other asset, must be appropriately protected.

This Cyber Security Incident Response Plan outlines the procedures Procreation UK Limited uses to detect and respond to unauthorised access or disclosure of private information from systems utilised, housed, maintained or serviced by Procreation UK Limited more specifically, this plan defines the roles and responsibilities of various Procreation UK Limited staff with respect to the identification, isolation and repair of data security breaches, outlines the timing, direction and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

Procreation UK Limited also implements practices designed to proactively reduce the risk of unauthorised access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection and numerous other industry standard systems.

In the event of a cyber security incident, Procreation UK Limited staff have been trained to expeditiously deal with the matter. Procreation UK Limited staff are trained on a yearly basis to recognize anomalies in the systems they regularly utilise, and to report any such anomalies as soon as possible to the Incident Response Manager so the Incident Response Team can be mobilised. Throughout the year the Incident Response Team are kept up to date on the latest security threats and trained in modern techniques of incident remediation.

The availability and protection of the information resources managed by the systems we maintain is of paramount importance to our company and will always be a core value of our organisation.

DEFINITIONS

Cyber Security Incident -

A Cyber Security Incident is any event that threatens the confidentiality, integrity or availability of the information resources we support or utilise internally, especially sensitive information whose theft or loss may be harmful to individuals, our clients or our company.

Incident Response Team (IRT) -

The IRT is made up of experts across different fields in the organisation whose charge is to navigate the organisation through a Cyber Security Incident from the initial investigation, to mitigation, to post incident review. Members include an Incident Response Manager, technical hardware and networking experts, front-end software experts, communications experts and legal experts.

Incident Response Manager (IRM) -

The IRM oversees all aspects of the Cyber Security Incident, especially the IRT. The key focuses of the IRM will be to ensure proper implementation of the procedures outlined in the Cyber Security Incident Response Plan, to keep appropriate Incident Logs throughout the incident, and to act as the key liaison between IRT experts and the organisation's management team. At the conclusion of a Cyber Security Incident, the IRM will conduct a review of the incident and produce both an Incident Summary Report and a Process Improvement Plan.

Cyber Security Incident Log -

The Cyber Security Incident Log will capture critical information about a Cyber Security Incident and the organisations response to that incident, and should be maintained while the incident is in progress.

Incident Summary Report (ISR) -

The ISR is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Plan, including how the IRT followed the procedures and whether updates are required. The template for the ISR may be seen in Appendix A.

Process Improvement Plan (PIP) -

The PIP is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide recommendations for avoiding or minimizing the impact of future Cyber Security Incidents based upon the "lessons learned" from the recently-completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix B.

INCIDENT RESPONSE TEAM

INCIDENT RESPONSE MANAGER

Name: Matt Francis	Email: matt@procreation.tv
Work: 020 8977 5361	Mobile: 07970 563 101

TECHNICAL CONTACTS

Name: Graham Potter	Email: graham@procreation.tv
Work: 020 8977 5361	Mobile: 07855 255 316

Name: Dave Kimberley	Email: dave@krystal.uk
Work: 020 8050 1337	Mobile: 020 8050 1337

LEGAL COUNSEL

Name: Hasnath Ahmed	Email: hasnath@briffa.com
Work Phone: 020 7288 6003	Mobile: 020 7288 6003

COMMUNICATIONS SPECIALIST

Name : Andrew Somerville	Email : Andrew@hubbubwireless.com
Work Phone : 020 8977 5361	Mobile: 07834 778 758

ADDITIONAL MEMBERS

In addition to those individuals listed above, additional experts may be included on the IRT, depending upon the nature and scope of the incident. In particular, an additional software support expert from the team that supports the software in question may be necessary. These additional members will be chosen by the IRM.

INCIDENT MANAGEMENT PRINCIPLES

CONFIDENTIALITY

Investigation

During a Cyber Security Incident investigation, the IRM or members of the IRT will be gathering information from multiple computer systems and/or conducting interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Cyber Security Incident will be strictly confidential throughout the investigative process. All members of the Cyber Security Incident Response Team are trained in information security and data privacy best practices. At the conclusion of the investigative process, the IRM will brief the client on the relevant details of the incident and the investigation (see Briefing of Client Response Phase on page 12). During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

Affected Stakeholders

In the event the incident involves the unauthorised access or disclosure of confidential information, Procreation UK Limited will communicate information relevant to the incident as well as any additional requested information to which they have a right (e.g. specific records.) Procreation UK Limited does reserve the right to withhold certain information at the discretion of the IRM if that information may jeopardise current or future investigations, or pose a security risk to Procreation UK Limited or other entities.

In the event the incident involves information of an non-Procreation UK Limited stakeholder group, Procreation UK Limited will take appropriate steps to notify those entities as efficiently as possible.

In the event the incident is limited to Procreation UK Limited systems not containing sensitive or confidential information, it will be the discretion of Procreation UK Limited the client and the IRM whether or not to share information related to the incident with outside stakeholders.

Report Management

All reports generated during an investigation along with any evidence gathered will be stored and managed by the IRM. Any physical records will be stored in the IRM's office in a locked file. Any digital records will be stored on the internal company network in a network share only accessible by the IRM and approved company Administrators. That share will be backed up and stored in accordance with Procreation UK Limited regular backup procedures. In the event past records of incidents need to be reviewed, a written request must be made to the IRM that includes the requestor, the information requested and the reason for the request. The IRM will review the request and has the discretion to approve or deny any request. Incident summary information will always be made available by the IRM.

COMMUNICATION GUIDELINES

- Communication with the client will be via the IRM.
- Initial communication to affected stakeholders should occur as expeditiously as possible upon the identification of the incident. In some cases, this may include an initial communication (email, phone call) that simply states awareness of the issue. In any scenario Procreation UK Limited will inform the client within 24hrs of an incident.
- Updated communications will come from the Incident Response Manager.
- The clinet should be clearly informed by the Incident Management Team what information is public and what is internal/confidential.
- Any incoming news media calls and requests for information will be directed through Incident Response Team Communication Specialist. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from Procreation UK Limited or the client, whichever is deemed most appropriate..

CYBER SECURITY INCIDENT PHASES

IDENTIFY

Overview

All Procreation UK Limited staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity or availability of the information resources we support or utilise internally should immediately be reported to the IRM.

Incident Types

Types of cyber incidents that may threaten the organisation are:

- Unauthorised attempts to gain access to a computer, system or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorised access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, corruption or unauthorised distribution

Incident Symptoms

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content or activity
- Locally hosted websites won’t open or display inappropriate content or unauthorised changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed

ASSESS

Overview

Once anomalous activity has been reported, it is incumbent upon the IRM to determine the level of intervention required. Other members of the IRT may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion, the IRM will alert the entire IRT immediately so that the situation may be dealt with as expeditiously as possible.

Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been / are being / will be impacted?
- How wide spread is it?
- Which stakeholders are affected?

Documentation

Regardless of whether it is determined there is a security threat, the IRM will accurately document the scenario in a Cyber Security Incident Log. All Cyber Security Incident Logs will be stored in a single location so incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident
- Characteristics of the activity
- Date and time the potential incident was detected
- Nature of the incident (Unauthorised access, DDoS, Malicious Code, No Incident Occurred, etc.)
- Potential scope of impact
- Whether the IRT is required to perform incident remediation?

RESPOND

Client Briefing

Upon determining that a significant incident or breach has occurred, the client should be notified immediately. As additional information is uncovered throughout the investigation, the client should be briefed by the IRM so appropriate decisions, such as allocating additional staff or resources or hiring outside consultants can be made. Additionally, based on the incident, it will be incumbent on the client to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so. In any scenario the ICO (Information Commissioners Office) must be informed within 72hrs.
The client should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, applicable laws and the communication requirements of all parties involved.

Initial Response

The first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve measures up to and including immediately disconnecting particular workstations, servers or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas in order to define the entire scope of the incident.

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

Remediation and Recovery

Once the cause has been determined and appropriately isolated, the IRT will need to remove the vulnerabilities leading to the incident. This may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the IRM
- Closely monitor the systems once reconnected to the network

REPORT

Overview

Once the threat has been mitigated and normal operation is restored, the IRM will compile all available information to produce an accurate and in-depth summary of the incident in an Incident Summary Report (ISR). A copy of the ISR is located in Appendix A. Throughout the incident, the IRT will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the IRT to obtain any additional information that may be available to augment the logs and records kept throughout the process. Additionally, a record of all email complaints of breaches or unauthorised releases of data and their disposition in accordance with applicable data retention policies.

Report Contents

The Incident Summary Report (ISR) will include all pertinent information to the incident, but at minimum:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of emails, etc. where possible)

Timeframe

The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the IRT should be conducted immediately to ensure the greatest possible accuracy of information.

REVIEW

Post-Incident Review Meeting

After the conclusion of the incident, the IRM and possibly select members from the IRT will meet with the client to discuss the event in detail, review response procedures and construct a Process Improvement Plan (PIP) to prevent a reoccurrence of that or similar incidents. The compiled Incident Report constructed by the IRM will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented and findings discussed. The IRM will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan.

As a whole, the group will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

Process Improvement Plan

The IRM will draft a Process Improvement Plan (PIP) based on the results of this meeting. The plan should discuss any applicable items necessary to prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately. Areas of focus may include, but are not limited to:

- New hardware or software required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

APPENDIX A:

INCIDENT SUMMARY REPORT

INCIDENT SUMMARY

Type of Incident	
Date Incident Originated	
Date Incident Was Detected	
By Whom Was Incident Detected	
How Was Incident Detected	
Scope of Incident (Systems Affected)	
Date Incident Corrected	
Corrective Action Types (Training, Technical, etc)	

Summary of Incident Symptoms

Summary of Incident Type and Scope

Summary of Corrective Actions

Summary of Mitigation Processes and Internal Communication

Communications Log (Attach communications emails, synopsis for verbal communication)

Communication Date	Communication Type	Recipient(s)	Purpose

APPENDIX B:

PROCESS IMPROVEMENT PLAN

PROCESS IMPROVEMENT PLAN

Areas of Success Summary

Areas in Need of Improvement Summary

Recommended Improvements to Avoid Future Incidents

Recommended Improvements to the Cyber Security Incident Response Plan

Improvement	Timeframe	Cost

APPENDIX C: INCIDENT LOG

INCIDENT LOG

Incident Title

Incident Opened Date

Incident Description

Action / Event	Date / Time	Performed / Reported by	Details