Katholische
Kirchgemeinde Luzern

Informatik- und Kommunikationstechnologien (IKT)

Anwenderanweisung

Katholische Kirche
Stadt Luzern

Inhalt

1 Zweck und Geltungsbereich

Die IKT-Anwenderweisung dient zum Schutz der Daten der Katholischen Kirchgemeinde Luzern (KGLU). Die grosse Verbreitung der IKT in der KGLU hat zur Folge, dass unzulässige Veränderungen oder die Zerstörung von Daten zu einem Ausfall der Systeme führen. Dies kann sowohl einen finanziellen als auch einen Imageschaden verursachen. Der Schutz der Daten und der Informatik ist daher ausserordentlich wichtig.

In der vorliegenden Weisung wird der Umgang mit Daten, Geräten und Anwendungen (Programmen) in Bezug auf den Datenschutz und die Datensicherheit geregelt. Die Weisung ist für alle Benutzerinnen und Benutzer von IKT-Mitteln der KGLU verbindlich. Sie gilt auch für externe Partner.

In begründeten Fällen sind Ausnahmen von einzelnen der nachfolgenden Regelungen möglich. Sie bedürfen der schriftlichen Genehmigung der zuständigen IT-Verantwortlichen (EDV-Ausschuss) der KGLU.

2 Grundlagen (Gesetze/Vorgaben)

2.1 Datenschutzgesetz des Kantons Luzern

Als Organ im Sinn des kantonalen Datenschutzgesetzes (DSG) haben die KGLU und mit ihr die Mitarbeitenden und Vorgesetzten für die Sicherung von Personendaten, insbesondere vor Verlust, Fälschung, Entwendung sowie Kenntnisnahme, Kopieren und Bearbeiten durch Unbefugte, zu sorgen (§7 Abs.1 DSG).

2.2 Synodalgesetz zum Kirchlichen Datenschutz

Auf der Grundlage der Datenschutzgesetzgebung des Kantons Luzern gewährleisten die Kirchen den Datenschutz. Sie berücksichtigen zudem allfällige kirchliche Vorgaben. Das Bearbeiten sämtlicher Personendaten ist auf die Erfüllung der kirchlichen Aufgaben auszurichten, wie sie im staatlichen und kirchlichen Recht beschrieben sind.

2.3 Personalreglement (PR) der Katholischen Kirchgemeinde Luzern

Die KGLU regelt in ihrer Personalverordnung (§12) die Rechte und Pflichten der Mitarbeitenden und Massnahmen bei Verstössen gegen Anordnungen und Weisungen. Ebenfalls wird im Personalreglement der Umgang mit dem Datenschutz geregelt (§11).

3 Verhalten im Umgang mit IKT-Mitteln

3.1 Generell

Die Informatik- und Kommunikationsmittel (IKT) werden den Mitarbeitenden mit individuellen Rechten und Pflichten zur Verfügung gestellt. Die IKT-Mittel dürfen nur im Rahmen des vorgesehenen Einsatzes verwendet werden.

Die am Arbeitsplatz zur Verfügung gestellten IKT-Mittel sind in erster Linie für geschäftliche und im unternehmerischen Interesse liegende oder bewilligte Zwecke zu nutzen. Die Nutzung der Infrastruktur für private Zwecke ist erlaubt, soll sich aber auf das Minimum beschränken und ausserhalb der Arbeitszeit stattfinden.

Die Informatik- und Kommunikationssysteme der KGLU dürfen in keiner Art und Weise für widerrechtliche, rassistische, sexistische oder anderweitig unsittliche Zwecke genutzt werden.

3.2 Eigenverantwortung

Die Mitarbeitenden sind in ihrem Zuständigkeitsbereich zu einem verantwortungsvollen Umgang mit den IKT-Mitteln verpflichtet. Sie halten sich an die gesetzlichen Vorschriften und die internen Weisungen. In Zweifelsfällen wenden sie sich an die Vorgesetzten oder an den zuständigen IT-Verantwortlichen der KGLU.

3.3 Verhalten bei sicherheitsrelevanten Vorfällen

Die Mitarbeitenden sind verpflichtet, Probleme mit den IKT-Mitteln umgehen dem IT-Verantwortlichen zu melden.

Es ist den Mitarbeitern untersagt, bei sicherheitsrelevanten Vorfällen eigene Aufklärungsversuche zu unternehmen, da so unter Umständen wertvolle Zeit verstreicht bzw. der Schaden evtl. noch grösser wird.

4 Datenklassifizierung

Im Anhang wird die Methodik der Klassierung näher erläutert. Generell gilt:

- Dokumente, die nicht speziell klassiert sind, gehören zur Klasse 2 (nicht öffentlich).
- Die Dateneignerin bzw. der Dateneigner ist verantwortlich für die Klassierung der Daten und Dokumente in ihrem/seinem Zuständigkeitsbereich. Sie/er informiert die Mitarbeitenden über die Klassierung der genutzten Daten und Dokumente.

Klasse 1: Öffentlich: Daten sind öffentlich, die Verbreitung soll jedoch bewusst erfolgen.

Klasse 2: Nicht öffentlich (intern): Daten sind nicht öffentlich, unrechtmässig Verbreitung kann Personen beeinträchtigen oder wirtschaftlichen Schaden verursachen.

Klasse 3: Vertraulich: Daten und Dokumente , an deren vertraulicher Behandlung ein erhebliches Interesse besteht. Eine Veröffentlichung führt zu einem bedeutenden Schaden bei den betroffenen Personen oder Unternehmen. Zur Klasse 3 (vertraulich) gehören insbesondere Personendaten und Persönlichkeitsprofile gemäss Datenschutzgesetz des Kantons Luzern sowie die Beschlüsse des Kirchenrates der KGLU.

5 Umgang mit Daten

5.1 Clear-Desk

Grundsatz: Alle Informationen und Daten, gleich ob in elektronischer Form oder Papierform, sind vor unberechtigtem Zugriff zu schützen.

Für die KGLU gilt die „Clear-Desk-Policy“; das bedeutet, dass der Arbeitsplatz nur verlassen wird, wenn alle vertraulichen Daten (Klasse 3) unter Verschluss sind.

Folgende Regelungen gelten generell für die interne Datenbearbeitung:

- Mitarbeitende dürfen nur diejenigen Daten bearbeiten, die sie zur Erfüllung ihrer Funktion benötigen.
- Mitarbeitende tragen die Verantwortung für den Schutz der in ihrem Einflussbereich bearbeitenden Daten und sind für die Einhaltung der Vertraulichkeit besorgt.

- Computer sind beim Verlassen des Arbeitsplatzes zu sperren. Kann eine Sperrung nicht erfolgen, so ist der Raum, in dem sich das Gerät befindet, abzuschliessen.
- Magnetische, elektronische Datenträger und Papierdokumente sollen wenn immer möglich unter Verschluss aufbewahrt werden.
- Alle Datenträger sind bei der Entsorgung physisch zu zerstören (USB-Sticks und Bänder in Stücke brechen) oder der IT zur Entsorgung zu übergeben.
- Die Mitarbeitenden unterliegen der Schweigepflicht bezüglich Informationen, die sie während der Arbeit erhalten und bearbeiten. Diese Schweigepflicht gilt uneingeschränkt während der Dauer des Arbeitsverhältnisses sowie nach dessen Beendigung und ist zeitlich unlimitiert.

5.2 Datenspeicherung

Geschäftliche Daten sind auf den Servern der KGLU bzw. den Laufwerken der Bereiche (Laufwerk I:\, L:\, usw.) zu speichern. Das Speichern von Daten auf lokalen Laufwerken C:\ ist, da dieses Laufwerk nicht gesichert wird, nicht gestattet.

Private Daten dürfen nur auf dem persönlichen Netzlaufwerk (H:\) gespeichert werden. Allerdings sind diese auf ein Minimum zu beschränken (keine Datenspeicherung der privaten Installation). Das Speichern von privaten Daten auf das lokale Laufwerk C:\ ist bedingt möglich. Das Risiko trägt der Mitarbeiter.

5.3 Externe Datenbearbeitung

Die externe Bearbeitung (gilt auch für PC-Heimarbeit via RAS) von Daten muss durch den zuständigen IT-Verantwortlichen der KGLU bewilligt werden und muss wie folgt ausgeführt werden:

- Die externe Bearbeitung von Daten ist auf das notwendige Minimum zu reduzieren.
- Die Originale sensibler und einmalig vorhandener Akten und Daten verbleiben in jedem Fall innerhalb der KGLU.

5.4 Externe Datenbearbeitung auf privaten PCs / mobilen Geräten

Bei bewilligter länger dauernder externer Datenbearbeitung sind die Daten regelmässig auf einem lokalen Zweitmedium (z.B. USB-Stick oder externer Festplatte) und periodisch auf den Servern der KGLU zu sichern. Das lokale Zweitmedium ist sicher aufzubewahren.

Daten der Klasse 3 (Vertraulich) dürfen extern nur mit „RAS-Home“ oder auf verschlüsselten Datenträgern bearbeitet werden.

Auf mobilen Geräten der KGLU (Notebooks, Tabletts, Smartphones, USB-Sticks usw.) dürfen Daten der Klasse 3 nur verschlüsselt gespeichert bzw. transportiert werden.

Werden Daten der Klasse 3 gefaxt, muss der Empfänger/die Empfängerin bzw. der Sender/die Senderin anwesend sein. Die Vorlage oder die Sendung darf nicht unbeaufsichtigt gelassen werden.

Auf öffentlichen oder anderen Dritt-PCs (z.B. in Internetcafés) dürfen ausschliesslich Daten der Klasse 1 bearbeitet werden.

Daten bei denen sichergestellt werden muss, dass sie nachträglich inhaltlich nicht verfälscht werden, dürfen nur als PDF mit Passwort oder einer elektronischen Signatur verschickt werden.

Für PC-Heimarbeit genutzte Geräte sind angemessen gegen Viren und Nutzung durch unbefugte zu schützen.

6 Login und Passworte

Zur Identifikation der Mitarbeitenden für den Zugang zu den Systemen, Applikationen und Daten werden Benutzernamen und Passwort (Identifikationsmittel) eingesetzt. Der sorgfältige und bestimmungsgemässe Einsatz der Identifikationsmittel trägt wesentlich zum Datenschutz und zur Datensicherheit bei.

Die Mitarbeitenden sind verantwortlich für alle Handlungen, die durch sie oder in ihrem Anmeldenamen (Login) an den Systemen, Applikationen und Daten vorgenommen werden. Insbesondere gilt:

- Eigene Passwörter sind persönlich und dürfen ausschliesslich den Benutzenden bekannt sein. Sie dürfen niemandem mitgeteilt werden und müssen sicher abgelegt sein.
- Die Speicherung bzw. Hinterlegung eines Passwortes auf einem Internet-Browser ist untersagt.

Regeln für ein gutes, sicheres Passwort:

- Das Passwort muss eine Mindestlänge von acht Zeichen haben und wird alle drei Monate gewechselt.
- Es hat keine direkt zuordenbaren Zeichenketten aus dem privaten Umfeld (Vor-, Nachname, Ortschaften, Telefonnummern, Geburtstag, Autokennzeichen usw.).
- Es lässt sich nicht durch einfache logische Überlegungen aus früheren Passwörtern ableiten.
- Es kommt nicht in einem Wörterbuch vor.
- Es enthält Zahlen, kleine und grosse Buchstaben und Sonderzeichen (z. B. $-Zeichen).

Hinweis: Das Login-System ist so eingestellt, dass die Eingabe eines starken Passworts technisch erzwungen wird (Beispiel für ein starkes Passwort: 1PaxxW@rt_4You)

7 Umgang mit Hardware/Software

7.1 Hardware

Für die Erledigung der Aufgabe sind grundsätzlich die IKT-Mittel der KGLU einzusetzen. Private Hardware darf nicht an das Netzwerk oder an ein anderes IKT-Mittel der KGLU angeschlossen werden. Veränderungen an der Hardware dürfen nur durch den IT-Verantwortlichen der KGLU vorgenommen werden.

7.2 Software (Programme und Daten)

Sämtliche Installationen oder Modifikationen von Anwenderprogrammen erfolgt durch den IT-Verantwortlichen der KGLU. Alle in der KGLU eingesetzten Softwareprodukte müssen durch den IT-Verantwortlichen geprüft sein und autorisiert werden.

Es ist nicht erlaubt, auf den zur Verfügung gestellten IKT-Mitteln der KGLU private Software zu installieren (z.B. Software-Downloads aus dem Internet).

Es ist den Mitarbeitenden der KGLU untersagt, die eingesetzte Software zu kopieren, weiterzugeben oder zu Hause zu installieren. Aus Lizenzgründen ist auch eine Zweitinstallation zu Haus nicht erlaubt.

Ausnahmen erfordern die Zustimmung des IT-Verantwortlichen und der/des zuständigen Vorgesetzten.

8 Malware (Viren, Trojaner und Ransomware)

Daten aus externen und unbekannten Quellen (z.B. auf USB-Sticks, CDs) sind grundsätzlich nicht vertrauenswürdig. Dies gilt insbesondere auch für heruntergeladene Daten aus dem Internet sowie für E-Mails und deren Anhänge. Besteht ein Verdacht auf Virenbefall, ist die E-Mail bzw. die Datei umgehend zu löschen.

Dateianhänge (Attachments) in nicht vertrauenswürdigen E-Mails dürfen auf keinen Fall geöffnet werden. Das Anklicken von Links (Verbindungen zu Websites) in zweifelhaften Mails ist sehr gefährlich. Bereits durch einen Linkaufruf können schädliche Inhalte heruntergeladen werden.

E-Mail-Adressen können leicht gefälscht werden. Somit sind die Absenderangaben immer zu hinterfragen.

Auf unerwünschte Nachrichten (Spam) darf nie persönlich geantwortet werden. Kettenbriefartige Aufforderungen nach Weiterleitung von E-Mail an alle Bekannten und Kollegen sind zu ignorieren.

Das Antworten auf E-Mails, in denen aufgefordert wird, vertrauliche Informationen preiszugeben (Passwörter, Kreditkartennummern, Bankangaben usw.), ist zu unterlassen, selbst dann, wenn die Nachricht vertrauenswürdig erscheint oder angebliche Konsequenzen angedroht werden. Im Zweifelsfall die Vorgesetzte/den Vorgesetzten oder den IT-Verantwortlichen anfragen.

Die PCs der KGLU sind so konfiguriert, dass die Prüfung auf Viren automatisch erfolgt. Das Deaktivieren der Virenschutzmechanismen ist untersagt. Falls es trotzdem zu einer Virenverseuchung gekommen ist oder der Verdacht darauf besteht, ist der IT-Verantwortliche unverzüglich zu informieren.

Massnahmen der Mitarbeitenden zur Untersuchung und Entfernung einer allfälligen Virenverseuchung sind zu unterlassen. Das verseuchte Gerät darf bis nach der Klärung der Situation nicht mehr genutzt werden.

9 Onlinedienste (Internet und E-Mail)

9.1 Berechtigung für Onlinedienste

In der KGLU gehört der Internetzugang, sofern nicht anderslautende Weisungen der zuständigen Gremien vorliegen, grundsätzlich zur Basisausrüstung eines Arbeitsplatzes (persönliches Login).

9.2 Nutzung von Onlinediensten

Die Benutzenden verpflichten sich bei der Anwendung von Onlinediensten zur Wahrung der Verhältnismässigkeit der Nutzung.

Alle Informationen aus Onlinediensten sind grundsätzlich kritisch zu würdigen, da sie keinen Qualitätskontrollen unterliegen.

Aus dem Internet heruntergeladene Daten werden durch die Sicherheitssysteme der KGLU automatisch auf Viren geprüft.

Nutzung von Social Media (resp.? Sperrung von deren Nutzung)

Für die Benutzung von Onlinediensten dürfen nur die offiziellen Kommunikationsverbindungen benutzt werden. Der Einsatz von eigenen, separaten externen Verbindungen (z. B. via Modems) ist verboten.

9.3 Umgang mit E-Mail am Arbeitsplatz

9.3.1 E-Mail-Verwaltung bei Abwesenheit von Mitarbeitenden

Bei Abwesenheit dokumentieren die Mitarbeitenden ihre Abwesenheit mit dem Abwesenheitsassistenten von Outlook und weisen den Absender darauf hin, dass die E-Mails aus Sicherheitsgründen weder weitergeleitet noch durch Stellvertretende bearbeitet werden.

In Ausnahmefällen oder in direkter Abhängigkeit der Geschäftsprozesse definieren Mitarbeitende Stellvertretende mit abgestufter Berechtigung zur Einsicht und Weiterberarbeitung der geschäftlich eingehenden E-Mails.

Bei längeren Abwesenheiten infolge Krankheit einer/eines Mitarbeitenden hat die/der Vorgesetzte das Recht, einen temporären Zugriff mit eingeschränkten Rechten auf deren/dessen Postfach beim IT-Verantwortlichen zu beantragen.

Die automatische Weiterleitung von Daten an die private E-Mail-Adresse oder externe Stellen ist nicht zulässig.

9.3.2 E-Mail-Verwaltung beim Austritt von Mitarbeitenden

Vor dem Austritt haben mitarbeitende Personen den E-Mail-Verkehr zu den noch hängigen Geschäften (Dossiers) an ihre Vorgesetzten weiterzuleiten.

Die austretenden Mitarbeitenden haben die Übergabe sämtlicher Geschäftsdokumente an die KGLU schriftlich zu bestätigen.

Die austretenden Mitarbeitenden müssen ihre privaten E-Mails und/oder Dokumente auf private Datenträger speichern und von den Speichermedien der KGLU löschen.

Beim Austritt wird spätestens am letzten Arbeitstag der E-Mail-Account (wie alle anderen Accounts und Logins auch) durch den IT-Verantwortlichen gesperrt und der Briefkasten (wie die anderen Datenträger auch) gelöscht.

Absender, welche E-Mails an eine gesperrte E-Mail-Adresse schicken, werden automatisch informiert (Abwesenheitsassistent ist vor Austritt einzurichten), dass die Empfängeradresse hinfällig geworden ist. In der automatischen Antwort wird eine geeignete Ersatz-E-Mail-Adresse der KGLU angegeben.

9.4 Überwachung von Onlinediensten

9.4.1 Einleitung

Die KGLU stellt mit der Überwachung von Onlinediensten sicher, dass im Zusammenhang mit dem Gebrauch von Internet einerseits die Interessen und technischen Einrichtungen der KGLU nicht beeinträchtigt werden und andererseits die Persönlichkeitsrechte der Mitarbeitenden gewahrt bleiben. Die KGLU achtet und schützt im Arbeitsverhältnis die Persönlichkeit der Mitarbeitenden.

Die Überwachung erstreckt sich auf alle intern und extern mitarbeitenden Personen der KGLU.

Durch Benutzung des vernetzten Computers am Arbeitsplatz können folgende Interessen und technische Einrichtungen der KGLU beeinträchtigt werden:

- Speicherkapazität und Netzwerkbandbreite durch übermässige Internetnutzung.
- Daten- und Anwendungssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) durch Viren, Würmern, Trojanischen Pferden oder Installation von fremden Pro-grammen.
- Arbeitszeit und andere finanzielle Interessen (Produktivitätsverluste, Kostensteigerung für zusätzliche Mittel und/oder Leistungen, Netzkosten usw.).
- Weitere (rechtlich) geschützte Interessen, wie Geschäftsgeheimnisse oder Datenschutz.

Sowohl die Informatikdienste, die Vorgesetzten, der IT-Verantwortliche und der Datenschutzbeauftragte haben die Personendaten, die sie im Zusammenhang mit einer Protokollierung und Auswertung bearbeiten, durch angemessene technische Massnahmen gegen unbefugte Zugriffe zu schützen. Sie sorgen insbesondere für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Personendaten.

9.4.2 Vorrang technische Schutzmassnahmen

Die KGLU setzt in erster Linie auf technische Schutzmassnahmen gegen Missbrauch und technischen Schaden an ihren Einrichtungen.

Sie passt die technischen Schutzmassnahmen regelmässig dem Stand der Technik an. Die Anpassung erfolgt auch nach jeder technischen Störung.

Die KGLU informiert die Mitarbeitenden über die mit der Benutzung von vernetzten Computern verbundenen Gefahren.

Die KGLU verzichtet auf den Einsatz von Spionprogrammen.

9.4.3 Protokollierung der Internetaktivitäten

Zur Kontrolle der Einhaltung der vorliegenden IKT-Anwenderanweisung protokolliert die KGLU die Internetaktivitäten. Die KGLU verpflichtet die mit der Protokollierung beauftragten Informatikdienste, die Vertraulichkeit der Protokolle zu respektieren.

Die automatisierten Systemauswertungen protokollieren folgende Informationen:

- Account
- Aufgerufene Webseiten
- Zeitraum, in welchem die Aktivität stattfand
- Datenvolumen Download/Upload und Anzahl „Clicks“

Der KGLU obliegt keine gesetzliche Aufbewahrungspflicht im Zusammenhang mit Protokollierungen. Zu Beweissicherungszwecken werden die Protokolle für den laufenden und die drei vorangegangenen Monate aufbewahrt.

Im Rahmen von Sanktionsverfahren gemäss städtischem Personalrecht dürfen sie bis zum rechtskräftigen Abschluss des Verfahrens aufbewahrt werden. In einem gerichtlichen oder Strafverfolgungsverfahren gelten die entsprechenden prozessrechtlichen Aufbewahrungsvorschriften.

9.4.4 Technische Protokollierung

Die Informatikmittel führen Protokollierungen über die wichtigsten durchgeführten Aktivitäten durch. Die Protokolldateien werden automatisch durch die IT-Systeme erstellt. Sie werden in der Regel für sechs Monate aufbewahrt.

Die Protokollierung definiert sich als fortlaufende Aufzeichnung der Randdaten „wer“, „was“, „wann“ und findet in der KGLU an folgenden Stellen statt:

- Auf der Ebene des Internet werden Protokollierungen, bestehend aus der UserLogin („wer“), der Zeitangabe („wann“) und der abgerufenen URL („was“), generiert. Obschon die URL ein Randdatum ist, kann der abgerufene Inhalt in der Regel nachträglich wieder hergestellt werden.
- Beim Zugriff auf Intranetdienste besteht die Protokollierung aus dem Benutzernamen (UserLogin, „wer“). Die Zeitangabe („wann“) wird ebenfalls protokolliert sowie der Gegenstand („was“) wie Ein- und Ausloggen, Ausdrucken, Applikationsabruf usw.

9.4.5 Auswertungen

Der IT-Verantwortliche ist vom Kirchenrat beauftragt und berechtigt, zur Kontrolle der Umsetzung dieser Weisungen die eingesetzten Informatiksysteme periodisch zu überwachen und die Wirksamkeit der Massnahmen zu kontrollieren.

Es werden summarische Auswertungen in anonymer bzw. pseudonymer Form erstellt. Eine personifizierte Einzelauswertung erfolgt nur dann, wenn die anonyme bzw. pseudonyme Auswertung einen Missbrauch oder einen Verdacht auf Missbrauch feststellt, oder aber eine Vorgesetzte/ein Vorgesetzter dem IT-Verantwortlichen begründeten Verdacht auf Missbrauch gegenüber eigenen Mitarbeitenden glaubhaft machen kann. Bei festgestelltem Missbrauch oder bei begründetem Verdacht auf Missbrauch wird die Benutzergruppe darauf aufmerksam gemacht, dass fortan eine gezielte Überwachung vorgenommen wird oder dass fehlbare Anwenderinnen und Anwender persönlich ermittelt und disziplinarisch bestraft werden.

Als Missbrauch versteht die KGLU eine Verletzung der Nutzungsregelung gemäss dieser Weisung. Mit der Auswertung der Protokolle sind die Informatikdienste beauftragt. Das Resultat der Prüfung wird dem IT-Verantwortlichen vorgelegt. Er prüft und entscheidet, ob Verstösse gegen die Nutzungsvorschriften festgestellt wurden. Als missbräuchlich gelten übermässiger Datenverkehr und unzulässige Zugriffe auf das Internet (siehe dazu Kap. 9.4.5.2).

9.4.5.1 Störung der IT-Systeme

Manifestiert sich eine Störung der IT-Systeme trotz technischer Schutzmassnahmen, können bei der Suche nach den Ursachen die Protokolle beigezogen werden.

Ist die Ursache der Störung auf einen Missbrauch durch mitarbeitende Personen zurückzuführen, können diese gemäss Kap. 10 dieser Weisung zur Rechenschaft gezogen werden.

9.4.5.2 Andere Fälle

Wird ein Missbrauch festgestellt, so können falls nötig die entsprechenden Protokolle oder deren Auswertungen beigezogen werden. Bei erwiesenem Missbrauch können Sanktionen ergriffen werden.

Die personifizierten Auswertungen mit missbräuchlichen Nutzungen werden als Beweismittel gesichert. Es erfolgt eine Information an die Vorgesetzte/den Vorgesetzten.

Wenn eine Straftat durch Auswertung der Protokolle oder durch andere Hinweise festgestellt oder vermutet wird, sichert die KGLU die entsprechenden Protokolle. Sie behält sich das Recht vor, Anzeige gegen die betroffenen Personen zu erstatten.

10 Sanktionen

Zuwiderhandlungen gegen die massgeblichen gesetzlichen Vorschriften und die vorliegende Weisung können geahndet werden. Im Wiederholungsfall oder bei vorsätzlicher bzw. grobfahrlässiger Missachtung dieser Weisungen liegt eine schwere Verletzung des Arbeitsvertrages vor, was gegebenenfalls zur Kündigung des Arbeitsvertrages führen kann. Zusätzlich besteht Schadenersatzpflicht bzw. Haftung für entstandene und noch entstehende Schäden. Vorbehalten bleibt die Strafanzeige.

11 Gültigkeit

Diese Weisung tritt per sofort in Kraft.

Luzern, 1. Januar 2018

Kirchenrat der Kath. Kirchgemeinde Luzern

Susanna Bertschmann	Peter Bischof
Kirchgemeindepräsidentin	Geschäftsführer