

CHURCH SAFETY AND SECURITY RISK ASSESSMENT

A Beginner-Friendly Template for Churches and Ministries

Plain language. Worked examples. Built for volunteer leaders.

Church Name	_____
Assessment Date	_____
Completed By	_____
Next Review Date	_____
Approved By (Pastor / Board)	_____

How to Use This Document

Most churches don't have a dedicated security team. This document is written for the volunteer or staff member who has been asked to "put together a safety plan" and isn't sure where to start. You don't need to be a security professional, and you don't need any special software.

The goal isn't to make your church feel like an airport. The goal is to be thoughtful and prepared — so that your people, your ministry, and the vulnerable in your care are protected.

What is a risk assessment?

A risk assessment is a structured way of answering three questions:

1. What could go wrong in our church or ministry?
2. How likely is each problem, and how bad would it be?
3. What are we going to do about it?

That's it. Everything else is just detail.

How long will this take?

For a typical church (congregation of 50–500), expect 6–10 hours spread over two to four weeks. Don't try to do it all in one evening. Walk through one section at a time, talk to the people who know each ministry, and pray over the decisions you're making.

Who should be involved?

- A pastor or staff member with authority to approve changes
- A board/elder/deacon representative
- The children's or youth ministry leader (this is essential — child safety is a core concern)
- The facilities or maintenance person who knows the building inside out
- Someone who handles offerings, finances, or giving records
- If possible, a member of the congregation with relevant professional experience (law enforcement, medical, IT, insurance, legal)

If your congregation is small, the same person may wear several of these hats — that's fine. Just make sure each perspective is represented.

The sections in this document

- Section 1 — What You're Protecting: People, ministries, property, and information.
- Section 2 — Protecting Children and Vulnerable People: The most important section — read it first.
- Section 3 — What Could Go Wrong: Threats that churches commonly face.
- Section 4 — How to Score Risks: A simple 1–5 scale.
- Section 5 — The Risk Register: The main worksheet.
- Section 6 — What to Do About Each Risk: Reduce, Transfer, Avoid, or Accept.

- Section 7 — Safety Checklists: Quick yes/no checks for the main areas.
- Section 8 — Emergency Response Basics: What to do when something actually happens.
- Section 9 — Keeping This Living: How to make sure it doesn't end up in a drawer.

A note on spirit: This document might feel cold or corporate in places. That's the nature of checklists. But the reason we do this work isn't fear — it's love. Good preparation is a way of caring for the people God has entrusted to you. Keep that in mind when the forms start to feel impersonal.

Section 1 — What You're Protecting

Before you can protect things, you need to know what things you have. Churches have a wider range of assets than most businesses — from sanctuaries to sensitive pastoral counseling notes to Sunday morning cash offerings.

The six categories of church assets

Category	What it means	Examples at a typical church
People (highest priority)	Every person on your property — especially children, youth, and vulnerable adults.	Congregation during services, children in Sunday school, youth group members, elderly members, visitors, staff, volunteers.
Ministries and activities	The programs and events where ministry actually happens.	Worship services, Sunday school, youth group, small groups, food pantry, counseling, mission trips, weddings, funerals, special events.
Facilities	The physical building and grounds.	Sanctuary, classrooms, nursery, fellowship hall, kitchen, offices, parking lot, playground, parsonage, cemetery.
Money and giving	Funds the church handles, receives, or holds.	Offering collections, bank accounts, petty cash, benevolence funds, online giving, designated donations, building fund.
Information and records	Data the church keeps, some of which is very sensitive.	Member directory, giving records, background check files, pastoral counseling notes, baptism/marriage records, children's program rosters and medical info.
Equipment and technology	Tools and systems that support ministry.	Sound system, livestream equipment, computers, phones, church management software, website, Wi-Fi, vehicles (church van/bus).

Worksheet: Your asset inventory

Fill in the most important items in your church. You don't need to list every chair — focus on things where loss, damage, or harm would be a real problem. Aim for 20–30 entries total.

#	Category	Asset	Why it matters (what happens if harmed?)	Responsible person
1	People	Children in Sunday school & nursery	Direct harm to a child; devastating trauma to family; legal liability; loss of community trust	Children's Ministry Director
2	Information	Member giving records	Privacy violation; loss of donor trust; potential tax/legal issues	Church Treasurer
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

The yellow rows are examples. Replace them or add more as needed.

Section 2 — Protecting Children and Vulnerable People

Read this section first. For a church, child protection is not one risk among many — it is the most important category of risk you will address. The harm that can come from a failure here is devastating to victims, to families, to your ministry, and to the witness of Christ in your community.

The non-negotiable baseline

These are the minimum standards widely recommended by child protection experts, insurers, and denominational guidelines. If you can't meet these, the risk to children is unacceptably high, and addressing these should come before anything else in this document.

Mark each item honestly:

✓	Minimum standard	In place?
<input type="checkbox"/>	Background checks are completed on every staff member and volunteer who works with children or youth, before they begin.	
<input type="checkbox"/>	Background checks are renewed on a regular schedule (every 2–3 years is common).	
<input type="checkbox"/>	A written child protection policy exists and every children's or youth worker has read and signed it.	
<input type="checkbox"/>	The "two-adult rule" is followed — no child is ever alone with a single adult in a closed room.	
<input type="checkbox"/>	There is a waiting period (often 6 months of regular attendance) before anyone can volunteer with children.	
<input type="checkbox"/>	Classroom doors have windows or are kept open, so interactions are visible.	
<input type="checkbox"/>	Bathroom and diapering procedures are written, known, and followed.	
<input type="checkbox"/>	Children are only released to authorized parents or guardians (check-in/check-out system).	
<input type="checkbox"/>	Every children's/youth worker has completed training in recognizing and reporting abuse.	
<input type="checkbox"/>	Everyone knows how to report a concern — internally AND to civil authorities (mandatory reporting).	
<input type="checkbox"/>	Pastoral counseling with minors follows the same visibility rules as other children's ministry.	
<input type="checkbox"/>	Youth ministry events (retreats, lock-ins, trips) have clear supervision ratios and overnight rules.	

✓	Minimum standard	In place?
<input type="checkbox"/>	Electronic communication between adults and minors follows written guidelines (no private messaging, parents copied, etc.).	
<input type="checkbox"/>	A way exists for a child, parent, or volunteer to report a concern anonymously.	

If you cannot check a box above

That item becomes an automatic High or Critical risk in your risk register (Section 5). Don't soften the scoring to feel better about it. The right response to a gap in child protection is to fix it, not to hope nothing goes wrong.

Vulnerable adults

The same principles apply to ministries involving vulnerable adults — people with developmental disabilities, dementia, acute mental illness, or in crisis situations. Background-checked workers, visibility, the two-adult rule, and clear reporting channels all apply.

Mandatory reporting

Most US states require clergy and/or church workers to report suspected abuse of children to civil authorities. This is a legal obligation, and in most cases it takes precedence over pastoral confidentiality. Know your state's specific laws. Post the child protection services number somewhere every volunteer can find it. Never attempt to investigate a suspicion internally before reporting — that is not your role, and delay can cause serious harm.

Helpful resources

- GuideOne, Church Mutual, Brotherhood Mutual, and other church insurers publish free child protection resources.
- MinistrySafe, Protect My Ministry, Plan to Protect, and similar organizations offer training and background check services.
- Your denomination (if applicable) likely has official child protection guidelines — follow them.
- Darkness to Light (d2l.org) offers free and low-cost training for churches on recognizing abuse.

Section 3 — What Could Go Wrong (Threats Churches Face)

Threats to a church fall into a few broad categories. You don't need to worry about every one equally — some will matter more based on your location, size, and ministries. Read through and mark what applies.

Harm to children or vulnerable people

- Abuse by a staff member, volunteer, or visitor (covered in detail in Section 2).
- An unauthorized adult gaining access to children's areas.
- A child being released to the wrong person.
- A medical emergency where allergies or conditions weren't known by workers.
- A child being injured on playground equipment or during youth activities.

Violence or disruption during services or events

- A disruptive or mentally distressed person entering a service.
- Domestic violence spilling into the church (custody disputes, angry spouses).
- An active shooter or violent attacker — rare but severe; many churches now have a plan.
- Hate-motivated attacks — especially relevant if your congregation is ethnically, racially, or religiously targeted.
- Theft during a service when offices and bags are unattended.

Financial risks

- Theft of the offering (from the collection, the counting room, or the safe).
- Embezzlement by a staff member or volunteer with financial access.
- Fraud — fake invoices, impersonation of the pastor to request wire transfers, or scams targeting the elderly in the congregation.
- Misuse of designated funds (using benevolence money for general operations, etc.).
- Credit card fraud on online giving or bookstore sales.

Facility and safety risks

- Fire — kitchens, candles, electrical issues, storage of flammables.
- Slip, trip, and fall injuries — especially in winter, on stairs, or during setup/teardown.
- Medical emergencies during services — heart attack, stroke, seizure, allergic reaction.
- Kitchen or food service injuries and food safety issues.
- Vehicle accidents involving the church van, bus, or volunteer drivers.
- Weather — tornado, severe thunderstorm, flooding, extreme heat or cold during an outdoor event.
- Utility failure during a service (power outage, no heat in winter).

Cyber and information risks

- Phishing emails impersonating the pastor, asking a staff member or volunteer to buy gift cards or send money.
- Ransomware locking the church's computer files or database.
- Weak or shared passwords on church management software.
- Giving or member data exposed through a vendor breach.
- Livestream hijacking, zoom-bombing, or inappropriate content appearing on screens.
- A stolen laptop with counseling notes or member records.

Reputation and spiritual harm

- A leader's moral failure becoming public without a plan.
- Inappropriate social media behavior by staff or volunteers.
- A member or former member publicly attacking the church.
- A credible allegation — handled badly — causing compounding harm.

Compliance and legal

- Failure to meet mandatory reporting obligations.
- Improper employment practices (classifying workers, wage issues, background check laws).
- Tax compliance issues (proper handling of designated gifts, housing allowances, 1099s).
- Copyright issues with music, livestream, or media use (CCLI, sync licenses, etc.).
- Data privacy laws (HIPAA may apply to some counseling; state privacy laws increasingly touch churches).

Your specific threats

Think about your church's particular situation. Is your building historic and hard to secure? Are you in a rural area with long emergency response times? Do you run a preschool or daycare? Do you serve meals to the community? Do you have a controversial public stance that draws opposition? Write these in the margin or add them to the threat list in your register.

Section 4 — How to Score Risks

To compare risks, you need a consistent scoring method. Use a 1–5 scale for two things:

4. Likelihood — how likely is this to happen in the next year?
5. Impact — if it did happen, how bad would it be?

Multiply them to get a risk score from 1 to 25. Higher = more urgent.

Likelihood scale

Score	Label	Plain meaning	Rough rule of thumb
1	Rare	Would be surprising.	Less than once every 5 years.
2	Unlikely	Could happen, but probably won't.	Once every 2–5 years.
3	Possible	Might happen from time to time.	Roughly once a year.
4	Likely	Expect it this year.	Several times a year.
5	Almost certain	Already happens or will soon.	Monthly or more.

Impact scale

For a church, impact means more than money. Spiritual, relational, and mission impact matter just as much. Consider the worst plausible case.

Score	Label	What this looks like at a church
1	Minimal	Minor nuisance. Handled within a day. No lasting effect. Example: a small cash discrepancy that's quickly resolved.
2	Minor	Noticeable disruption. Some people affected. Example: a water leak damages carpet in a classroom; a few members are frustrated.
3	Moderate	Significant disruption or harm. Multiple people or families affected. Example: a minor injury on church property; a data breach of member emails; a week without the sound system.
4	Major	Serious injury, significant theft, major legal exposure, or a lasting blow to the church's witness. Example: a serious injury at a youth event; embezzlement of \$50,000; a ransomware attack that takes the church offline for weeks.
5	Catastrophic	Loss of life, severe harm to a child, or an event that could end the church. Example: abuse of a child on church property; an active attacker

Score	Label	What this looks like at a church
		during a service; a fire that destroys the building; a scandal involving leadership that splits the congregation.

The risk matrix

Multiply Likelihood × Impact. Use the color to figure out how urgent it is.

	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Likelihood 5	5	10	15	20	25
Likelihood 4	4	8	12	16	20
Likelihood 3	3	6	9	12	15
Likelihood 2	2	4	6	8	10
Likelihood 1	1	2	3	4	5

What the colors mean

Color	Score	What to do
Low	1–4	Acceptable. Note it, keep practicing good habits.
Medium	5–9	Worth addressing. Plan improvements within 6 months.
High	10–15	Needs action. Assign an owner and a deadline within 1–3 months.
Critical	16–25	Stop and fix. Escalate to pastor and board. Work on it this week.

A worked example

Risk: A volunteer who hasn't completed a background check is asked to cover a Sunday school class when a regular teacher calls out sick.

Likelihood = 4 (Likely). With no written backup system, last-minute substitutions happen several times a year. Good-hearted volunteers step in under pressure.

Impact = 5 (Catastrophic). An unscreened adult alone with children is the single greatest predictor of harm. Even if this particular volunteer is trustworthy, the pattern is unacceptable.

Risk score = 4 × 5 = 20 (Critical). Stop and fix this week. Build a pre-screened substitute list. Never run a class under-staffed rather than pulling in an unscreened adult.

Section 5 — The Risk Register

This is the main worksheet. For each risk you care about, fill in one row. Start with maybe 12–20 of the most important ones.

How to fill in each column

- ID — Just a number (R-01, R-02, etc.).
- Risk description — One sentence: "What could happen, to whom or what, caused by what."
- Category — People, Money, Facility, Information, Cyber, Ministry, Reputation, etc.
- Likelihood (1–5) and Impact (1–5) — Use the scales in Section 4.
- Score — Likelihood × Impact.
- Existing safeguards — What you already do about it (locks, training, policies, insurance, etc.).
- Action — What you plan to do from Section 6 (Reduce, Transfer, Avoid, Accept).
- Owner — Who is responsible. For churches, this is often a specific staff member or a standing committee, not a vague "the leadership team."
- Target date — When the action will be complete.

Tip: Don't get stuck trying to perfect each score. If you can't decide between a 3 and a 4, pick one and move on. You can refine it later.

Risk register worksheet

Three example rows are filled in (yellow). Replace them with your own, and add rows as needed.

ID	Risk description	Category	Existing safeguards	L	I	Score	Action	Owner	Due
R-01	Unscreened volunteer covers a Sunday school class at the last minute	People / Children	Verbal policy only; no written sub list	4	5	20	Reduce — build pre-screened sub list	Children's Ministry Director	30 days
R-02	Sunday offering counted by a single volunteer in a closed room	Money	Trusted volunteers; locked office	3	3	9	Reduce — two-person rule, tamper-evident bags	Treasurer	60 days
R-03	Staff member tricked by email pretending to be the pastor asking for gift cards	Cyber / Money	None specific	4	3	12	Reduce — verbal verification rule, staff training	Office Manager	90 days
R-04									
R-05									

ID	Risk description	Category	Existing safeguards	L	I	Score	Action	Owner	Due
R-06									
R-07									
R-08									
R-09									
R-10									
R-11									
R-12									
R-13									
R-14									
R-15									
R-16									
R-17									
R-18									

L = Likelihood, I = Impact, Score = L × I.

Section 6 — What to Do About Each Risk

For every risk, you have four options. There's no "right" answer — it depends on the cost, severity, and mission of your church.

Option	What it means	When to use it	Church example
Reduce	Put controls in place to make it less likely, less severe, or both.	The default answer for most risks.	Require two unrelated adults to count the offering.
Transfer	Shift the risk through insurance, outsourcing, or partnering with someone better equipped.	When the impact is big but your church can't cost-effectively reduce it further alone.	Carry church liability insurance including abuse and molestation coverage; use a payroll service for staff payroll.
Avoid	Stop doing the activity that creates the risk.	When the activity isn't essential and the risk is high.	Stop overnight youth events in private homes; use a public retreat center instead.
Accept	Acknowledge the risk and decide to live with it.	Only for low-scoring risks, or where the cost of treatment clearly outweighs the problem.	Accept that the parking lot will occasionally have minor fender-benders during busy services.

A word on insurance

Churches tend to be either under-insured or poorly-insured. Before you assume "we have insurance so we're covered," talk to your insurance broker about:

- Abuse and molestation coverage (often a separate policy or rider with limits lower than you'd expect).
- Directors and officers (D&O) coverage for your pastor, elders, and board.
- Cyber liability — many older church policies don't include this.
- Sexual misconduct allegations — coverage, limits, and legal support.
- Coverage for mission trips, youth trips, and off-site events.

Documenting accepted risks

Whenever you accept a risk that's Medium or higher, write down who made the decision and why.

The board minutes are a good place. If something goes wrong later, you want evidence that the church's leadership considered the risk carefully and made a reasoned decision — not that it was ignored.

Action plan worksheet

For every High and Critical risk, fill in one row with the specific actions you're going to take.

Risk ID	Action to take	Expected outcome	Owner	Due date
R-01	Build pre-screened substitute teacher list; written "never run a class alone" policy; pastor to review monthly.	Reduce likelihood from 4 to 1.	Children's Ministry Director	30 days from today

Section 7 — Safety Checklists

Walk through each list. A blank box is a signal that you may have an elevated risk. Use these checklists as a gut-check alongside the risk register.

Children's and youth ministry

- Every children's/youth worker has a current background check on file.
- A written child protection policy exists and every worker has read and signed it.
- The two-adult rule is followed, always. No exceptions.
- Check-in/check-out system releases children only to authorized adults.
- Classroom doors have windows or are kept open.
- Restroom procedures are written and followed.
- Every worker knows the mandatory reporting process and phone number.
- Medical info (allergies, conditions, emergency contacts) is accessible to workers but kept private.
- Youth trips have written parent consent, emergency contacts, and adequate supervision ratios.
- Electronic communication with minors follows written guidelines (parent copied, no private DMs).

Sunday / worship service safety

- A designated safety or security team is present during services.
- At least one member of the safety team has basic first aid / CPR training.
- An AED is on site and people know where it is.
- Exits are clearly marked, unobstructed, and known by ushers.
- A plan exists for a disruptive or distressed person entering a service.
- A plan exists for a medical emergency during a service.
- A severe weather plan is known by ushers and leadership.
- Greeters are trained to notice unusual behavior without being confrontational.
- Outside doors are monitored or locked after services start (balancing welcome with safety).
- A way exists to discreetly contact law enforcement during a service if needed.

Money and giving

- Two unrelated people handle and count the offering — never one alone.
- Offerings are secured in a locked safe or bank deposit the same day.
- Tamper-evident bags or sealed containers are used for cash.

- Bank deposits are made by varying people on varying routes/times.
- Financial records are reviewed at least quarterly by someone outside the treasurer role.
- An annual audit or financial review is performed.
- Designated funds are tracked separately from general operations.
- Large payments (over a set threshold) require two signatures or dual approval.
- Verbal verification is required before any wire transfer, gift card purchase, or unusual payment request, even if the request appears to come from the pastor.
- Online giving platform has strong security (MFA on admin accounts, limited access).

Building and facilities

- Exterior doors are secured when the building is unoccupied.
- Keys and access fobs are tracked; returned when someone leaves a role.
- Fire extinguishers are inspected annually and accessible.
- Smoke and carbon monoxide detectors work and are tested.
- The kitchen has clear safety rules and a first aid kit.
- Playground equipment is inspected regularly.
- Snow/ice removal is handled promptly in winter.
- Parking lot lighting is functional.
- Cleaning supplies and chemicals are stored away from children's areas.
- Insurance policies are current and coverage limits are reviewed annually.

Information and technology

- Every staff member and key volunteer has their own login — nobody shares accounts.
- Multi-factor authentication is on for email, giving software, and church management software.
- Passwords are managed with a password manager or meet minimum length (12+ characters).
- When someone leaves a role, their access is revoked the same week.
- Member and giving data is backed up regularly and restore has been tested.
- Sensitive records (counseling notes, background check results) are stored securely.
- Staff and volunteers have been trained on phishing and "fake pastor" scams.
- The church's Wi-Fi has a separate guest network.
- Livestream and video conferencing have settings that prevent hijacking.
- Old data is purged on a schedule (you don't need to keep everything forever).

Pastoral care and confidentiality

- Pastoral counseling with minors follows visibility rules (open door, window, etc.).
- Pastoral counseling records are stored securely and access is limited.
- Clergy know which state laws override confidentiality (mandatory reporting).
- A written policy exists for handling allegations against staff or leadership.
- Congregants know how to make confidential concerns known without going to the alleged offender's supervisor.
- Boundaries around personal relationships between pastors and parishioners are written and taught.

Section 8 — Emergency Response Basics

Even the best assessment won't prevent every incident. What matters just as much is what happens in the moments after. This section is a starting point — you may want to build a fuller emergency plan separately.

The three questions to answer for every emergency

6. Who is in charge? (The person who makes the call, not a committee.)
7. How do we communicate with the congregation and with first responders?
8. Where do people go, and who checks they're all accounted for?

Key emergency types and basic responses

Emergency	Immediate response	Next steps
Medical emergency	Call 911. Begin first aid / CPR if trained. Get the AED. Clear space.	Stay with the person until EMS arrives. Notify family. Document what happened.
Fire	Pull alarm. Call 911. Evacuate via nearest exit. Do not re-enter.	Account for everyone at the rally point. Check nursery and classrooms. Report to fire department.
Severe weather (tornado / severe thunderstorm)	Move everyone to pre-designated shelter area (interior rooms, no windows).	Stay until all-clear. Account for children with their check-in lists.
Disruptive person	Calmly engage; do not escalate. Guide away from children's areas. Safety team supports pastor/usher.	If escalating, call 911. Document incident. Consider whether a no-trespass notice is warranted.
Active attacker (rare but severe)	Run-Hide-Fight (as taught by DHS/FBI). Call 911 as soon as safe. Lock down children's areas.	After: reunification plan; cooperate with law enforcement; care for trauma.
Missing child	Lock exterior doors. Assign searchers. Check restrooms, classrooms, vehicles.	If not found in 10 minutes, call 911. Notify parents. Review check-in logs and video if available.
Suspected abuse of a child	Ensure the child is safe. Do NOT investigate internally. Do NOT confront the suspected adult.	Report to civil authorities (child protective services, police). Notify pastor and board. Follow written policy.
Financial fraud discovered	Stop the bleeding — freeze affected accounts, change passwords, preserve records.	Notify board, insurance, and if needed law enforcement. Don't confront suspected individual alone.

Emergency	Immediate response	Next steps
Cyber attack / ransomware	Disconnect affected computers from the network. Don't pay a ransom without guidance.	Call your IT provider and insurer. Restore from backup. Notify affected members if data was exposed.

Contact list

Fill in and keep this where volunteer leaders can find it.

Role	Name	Phone
Senior Pastor		
Safety/Security Team Lead		
Children's Ministry Director		
Church Office / Administrator		
Board / Elder Chair		
Insurance Agent		
IT Support / MSP		
Attorney (for the church)		
Local Police (non-emergency)		
Fire Dept (non-emergency)		
Child Protective Services		
Denominational Contact (if any)		

Section 9 — Keeping This Living

The biggest mistake churches make with safety plans is treating them as one-time projects. The value comes from using the plan to actually make decisions, and from revisiting it as things change.

A simple maintenance rhythm

How often	What to do	Why
Monthly	Check progress on action items.	Keeps improvements moving forward instead of sitting on a shelf.
Quarterly	Review the register for new or changed risks.	New ministries, new staff, new volunteers, and new threats all appear between annual reviews.
Annually	Full refresh of the whole document.	Re-score everything, re-check controls, get board sign-off.
After any incident	Update the relevant risk.	If something happened, your likelihood estimate was probably wrong. Learn from it.
After any big change	Reassess affected areas.	New building, new ministry, new staff in a key role, a significant event in the community.

Signs you're doing it right

- Leadership can name the top three risks without looking them up.
- Safety considerations come up naturally when planning new ministries or events.
- Volunteers know what to do when something unusual happens — they don't freeze.
- Action items from the last review actually got done.
- Children's workers feel supported, not suspected, by the protection policies.

Signs something's off

- The document looks exactly the same as last year.
- The same risks keep appearing year after year with no progress.
- Nobody outside the safety team has read it.
- Policies are written but not followed in practice.
- Volunteers roll their eyes when safety rules are mentioned.

Helpful resources for churches

- Your insurance provider — companies like Brotherhood Mutual, Church Mutual, GuideOne, and Philadelphia Insurance publish extensive free safety resources.

- MinistrySafe and Protect My Ministry — background checks and training programs designed for churches.
- The National Sheriffs' Association "Faith-Based Safety and Security Guide."
- Plan to Protect and Darkness to Light — training programs specifically for child protection.
- Your denomination (if applicable) — most have official child protection and safety guidelines.
- FEMA's "Guide for Developing High-Quality Emergency Operations Plans for Houses of Worship."

Sign-off

This assessment has been reviewed and approved by the church leadership. Action items have been assigned and will be tracked to completion.

_____ Name / Role	_____ Signature	_____ Date
_____ Name / Role	_____ Signature	_____ Date
_____ Name / Role	_____ Signature	_____ Date